

The cloud—services, computing and digital data

Emerging issues in media
and communications

Occasional paper 3

JUNE 2013

Canberra

Purple Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne

Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney

Level 5
The Bay Centre
65 Pirrama Road
Pymont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

© Commonwealth of Australia 2013

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Manager, Editorial Services, Australian Communications and Media Authority, PO Box 13112 Law Courts, Melbourne Vic 8010.

Published by the Australian Communications and Media Authority

Contents

Executive summary	1
Introduction	3
The cloud computing environment	4
What is cloud computing?	4
A diverse cloud market in Australia	6
Changing revenue models open opportunities for individual and small business cloud use	7
User data the new currency	8
Connected consumers in the cloud	9
Implications for regulatory settings	12
Economy-wide and industry-specific regulation	12
Cloud pressures communications regulation	13
New industry participants challenge industry-specific safeguards	14
Access to digital data just as important as access to networks	14
Changing profile of demand for public resources	15
Addressing barriers to cloud adoption	15
Security, privacy and data protections	15
Vendor lock-in, portability and ease of switching providers	17
Data sovereignty and redress	17
Regulatory strategies for confidence in the cloud	19
Confidence in standards and global governance for digital data	19
Facilitating industry cloud initiatives	20
Confident consumers	21
Conclusion	22

Executive summary

Cloud computing is an emerging and increasingly critical part of a modern economy. It is a general term for delivering hosted services over the internet to remotely store, process and share digital data. This paper is primarily concerned with the implications for regulatory settings of developments in cloud computing. It continues discussion of emerging issues in media and communications by the Australian Communication and Media Authority (the ACMA).

In Australia, large businesses and governments have been the primary users of cloud computing to date. Conditions for wider business and consumer adoption of cloud computing are now present in the Australian market, and the number of small businesses using cloud computing is increasing at a rapid rate. This is the result of the high take-up of smartphones that support cloud-enabled webmail, picture-sharing and social networking, and consumers creating and storing more and more digital data as part of their personal and social interactions.

Digital data has been widely described as the 'new oil' or currency of an information economy.¹ In this analogy, the providers of cloud computing are like the bank vaults of the 21st century, holding the keys to access personal and business data for transactions in an information economy. In contrast to the financial services sector that has well-established governance arrangements and enjoys a level of public confidence, there are many challenges for an emerging communications activity, such as cloud computing, in Australia.

Cloud computing shares many of the characteristics of other over-the-top (OTT) services. They include mobile applications and social networking services that operate globally, use fixed and mobile broadband access and combine features of infrastructure, service and content in one product. These characteristics also raise challenges for traditional regulatory models that have treated infrastructure, services and content separately.

Internationally, industry technical standards for cloud computing are still under development. Efforts are underway in other jurisdictions to standardise data protections and arrangements for the transfer or porting of data held in cloud computing. Within Australia, a mix of economy-wide and industry-specific regulatory measures are relevant to the operation of cloud computing. In May 2013, the government released the National Cloud Computing Strategy. The strategy recognises synergies between the National Broadband Network and cloud computing, and the important role for government in providing tools that small business, individuals and government agencies need to realise the promise of cloud computing. Given the potential advantages offered by cloud computing, there would be benefits in having cloud service issues considered within a single coherent regulatory framework.

The ACMA undertakes research to identify the dimensions of digital technology change and changes in the behaviour and expectations of digital citizens. Cloud computing is one the key technology developments that are having a significant impact on current regulatory settings. Consequently, they offer insights into how any

¹ Meglena Kuneva, European Consumer Commissioner, March 2009, cited [World Economic Forum Personal Data: The Emergence of a New Asset Class](#), p. 5.

future arrangements should be designed and will be an important input to the implementation of the strategy.

Introduction

Cloud computing is emerging as a significant development in contemporary communications and media because it becomes the storage and retrieval system for vast quantities of business and personal digital data. This data supports all transactions in an information economy.

While various forms of cloud computing have been available in the Australian market for around 20 years, adoption has been accelerating and the conditions are now present for a much wider take-up of cloud computing by consumers and small business (whether they are aware of it or not) as a wider variety of activities are undertaken online.

Providers of cloud computing services do not fit into the traditional communications industry definitions of network infrastructure, content or service providers and share many of the characteristics of other over-the-top services (OTT), such as mobile applications and social networking services. There are some unique challenges in how historical regulatory foundations of service portability; end-to-end connectivity and interoperability are translating into this new digital data ecosystem, along with consumer safeguards around privacy and personal communications.

This paper is the third in the series of occasional papers examining emerging issues in contemporary media and communications. Previous papers examined the apps market and developments in near-field communications.

This paper examines:

- > the cloud computing environment
- > the implications of cloud computing for current regulatory settings
- > barriers to cloud adoption in Australia
- > the suite of available regulatory and non-regulatory strategies to broaden business and consumer confidence in cloud computing.

The ACMA would welcome further discussion from interested parties on the following questions:

1. Are there other aspects of the cloud computing market and the use of cloud computing not covered in the discussion that should be considered by the ACMA?
2. Are there current barriers to further innovation occurring in cloud computing that need to be considered by the regulator?
3. In a globalised communications market, what are the most effective methods of supporting consumer confidence and productive engagement with cloud computing?
4. Are some regulatory or non-regulatory strategies better suited to facilitating further innovation and adoption of cloud computing while supporting consumer engagement with cloud computing?

Feedback on this paper can be sent to regframe@acma.gov.au.

The cloud computing environment

What is cloud computing?

Cloud computing is a general term for delivering [hosted services](#) over the internet to remotely store, process and share digital data. Smartphone capability and increases in computer processing power, in conjunction with faster broadband speeds, have been key drivers in encouraging the adoption of cloud computing. The increased reliability and speed of data transfer enables users to access services and applications more readily, outside the traditional office or home environment and across multiple devices.

There are three main categories of cloud computing, although the delineations between service categories are not always distinct, particularly as providers may offer more than one category of service type:

> **Infrastructure-as-a-Service (IaaS)**

IaaS providers offer data-centre capacity, processing resources and storage.² For example, Amazon web services provide application development and testing facilities, as well as disaster recovery and remote storage options.³

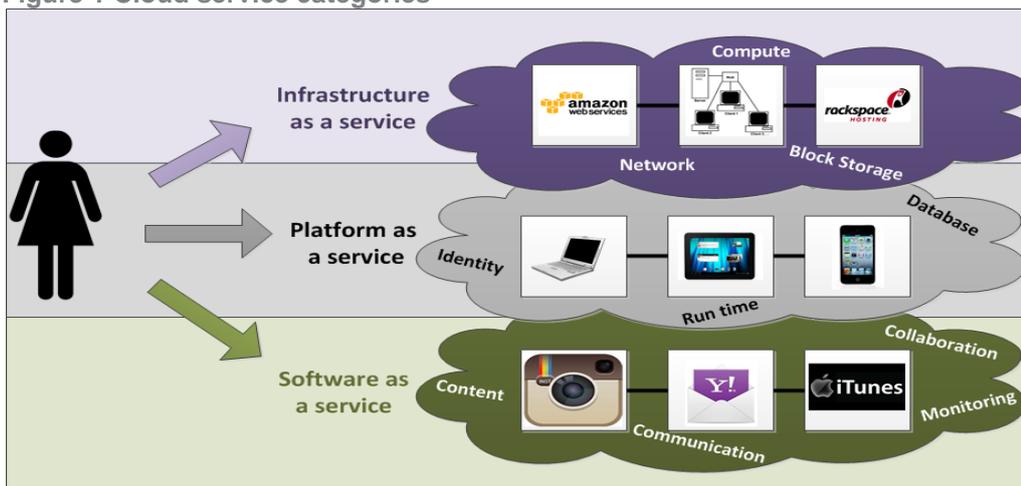
> **Platform-as-a-Service (PaaS)**

PaaS provides an environment for the development and hosting of applications.⁴ For example, Salesforce online application hosting services and platforms deliver website hosting and content delivery services.⁵

> **Software-as-a-Service (SaaS).**

Hotmail, Flickr and Instagram are examples of this service type.

Figure 1 Cloud service categories



² Ovum, The cloud computing landscape: a market scan, July 2009, p. 11.

³ *ibid.*, pp. 7–8.

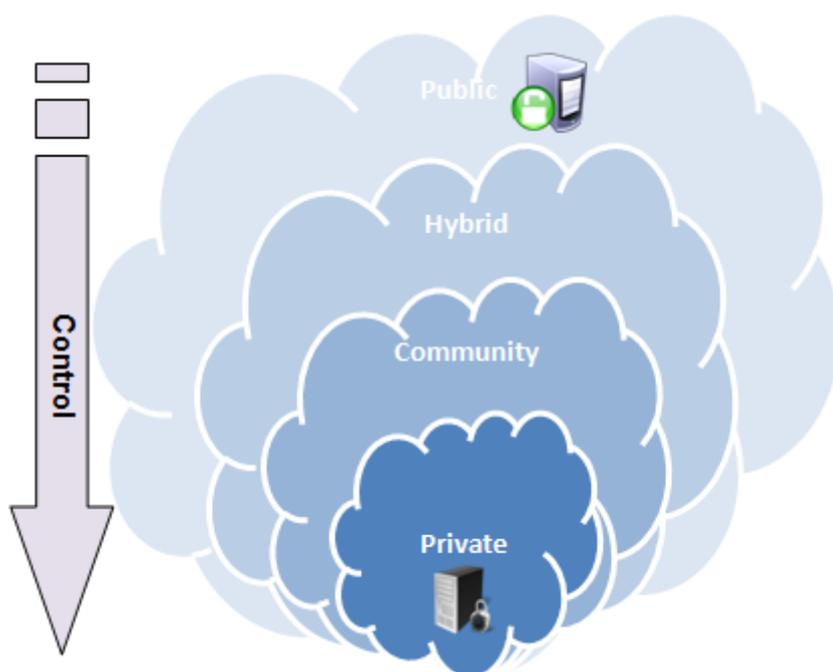
⁴ *ibid.*, p. 11.

⁵ *ibid.*, pp 7–8.

In the Australian market there are four main models of cloud in use with each of these service categories. They are:

- > **Private**—for the exclusive use of one organisation. It may be managed by the organisation or a third party and exist on-premises or off-premises.⁶ At present, this is the most common form of cloud computing used by business in Australia.⁷
- > **Public**—is made available to the general public or a large industry group and is owned by an organisation selling cloud computing.⁸ Services offered by Apple, Google and Amazon all fit into this category.
- > **Hybrid**—both private and public cloud models are used by a single organisation.⁹
- > **Community**—is shared by several organisations that wish to make use of a common cloud environment. The cloud may be managed by the organisations or a third party and may exist on premises or off premises.¹⁰

Figure 2 Main models of cloud computing in use in Australia



Cloud computing offers some key cost and efficiency benefits because of its service features that are:

- > **Dynamically scalable**—capacity is able to be scaled up and down. Cloud computing is enabling more complex and faster processing of tasks in an era where big data, and complex data analysis are becoming a fundamental part of doing business in the networked economy. The scalability of cloud computing allows end users to tailor services to meet the demands of the processing task being undertaken.
- > **Platform agnostic**—access across multiple devices and operating systems. This addresses consumer and business needs for mobility and multi-location access to

⁶ ATSE, [Cloud Computing: opportunities and challenges for Australia](#), p. 2.

⁷ KPMG, [Modelling the Economic Impact of Cloud Computing](#), p. 8.

⁸ ATSE, [Cloud Computing: opportunities and challenges for Australia](#), p. 2.

⁹ KPMG, [Modelling the Economic Impact of Cloud Computing](#), p. 8.

¹⁰ ATSE, [Cloud Computing: opportunities and challenges for Australia](#), p. 2.

information, services and applications. Cloud computing is a means of achieving these goals because they allow users access to their data across a range of devices. For example, webmail services allow users to access their email on smartphones, tablets, laptops and desktops. More recently, Microsoft's Office 365 and Skydrive and Google's Google App products all allow users to access their data from almost any internet enabled device

- > **Task centric**—services and products are able to meet the specific requirements of each task. For example, a firm doing data analysis can choose the number of servers it wants to dedicate to the task. With traditional communications technology firms, this would be limited by the number of physical servers they owned. Cloud computing services remove such technological limitations.
- > **Present no fixed costs**—such as ongoing licensing fees and equipment purchase costs, instead users pay-as-they-go for services. In addition, cloud computing provides end users (particularly small-to-medium enterprise) with greater economies of scale in their use and purchase of technology.¹¹

Figure 3 The cloud supports consumers' desire for mobility and access



A diverse cloud market in Australia

Cloud computing services are not a new concept; the communications market has seen the rise and fall of different models over the last 20 years. Webmail applications such as Hotmail and Yahoo mail, which were created in the late 1990s, are cloud computing services. Where software applications once operated from a server room down the hall, they are now based in data centres located anywhere in the world.¹²

Providers of cloud computing services do not fit into the traditional communications industry definitions of network infrastructure, content or service providers. Cloud computing shares many of the characteristics of other OTT services, such as mobile applications and social networking services, and are:

- > dependent on broadband access
- > global in terms of their market reach
- > have complex supply chains
- > often blur the distinctions between content and service
- > generally have multiple uses.

¹¹ KPMG, [Modelling the Economic Impact of Cloud Computing](#), p. 19.

¹² [Dan Hoffman, CEO, M5 Networks.](#)

The cloud industry is fragmented, with diverse product and service offerings that include:

- > server providers such as [Rackspace](#) and [Amazon Web Services](#)
- > file-sharing services like [Dropbox](#), and [Evernote](#)
- > web mail providers such as [Google](#), [Yahoo](#) and [Microsoft](#)
- > storage providers such as [Apple](#) and
- > sharing sites such as [Flickr](#).

In Australia, there are around thirty-eight cloud computing service providers providing on-demand information and communications technology services such as [Ninefold](#) and [Ultraserve](#).¹³ The last two years have seen overseas cloud service providers increasingly locating data centres in Australia (for example, IBM, Rackspace, Dell, Hewlett Packard and Amazon), or partnering with local businesses to provide locally based servers (Microsoft for example).

Combined with the rapid growth of OTT services, including social networking, app stores and content aggregators such as YouTube, the diversity of market participants and available product offerings introduces new issues for individuals and business in navigating this complex environment. For example, a storage provider may contract for service provision at a number of different geographical locations, and may also outsource its payment services. This can create issues for individuals and businesses when they need to alter their service arrangements, identify responsible parties or seek redress.

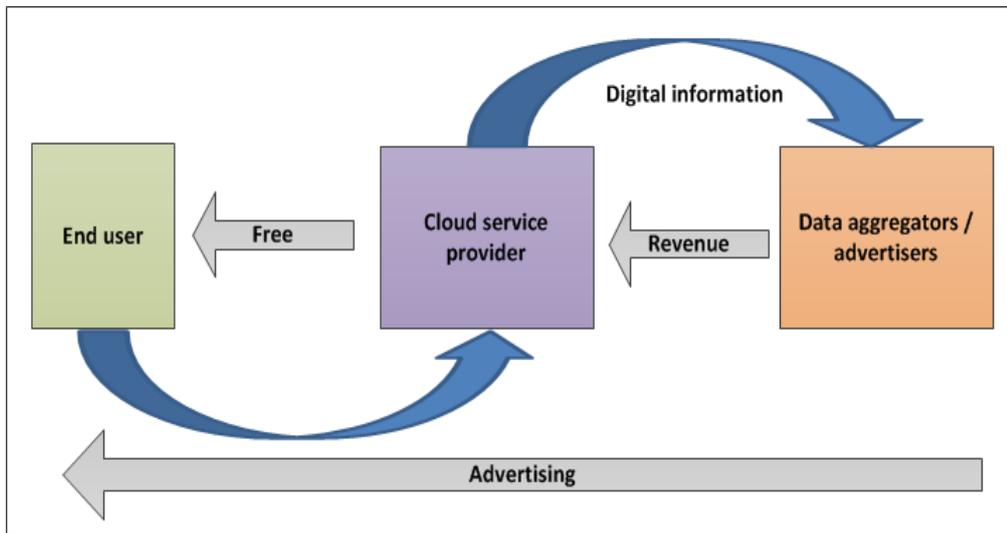
Changing revenue models open opportunities for individual and small business cloud use

Cloud service providers tend to focus their products and services on either the business enterprise or the public. While cloud service providers may offer products to a wide range of users, the focus on business enterprise or public end users shapes the methods of revenue generation adopted, and the importance of the activities associated with this. The two main models for revenue creation by cloud computing are:

- > **Freemium**—like Freemium offerings in the app market, this service is free to the end user, apart from any costs associated with using the service, such as bandwidth. Similar to the app market, cloud computing using this business model often generate income through other means not just through the up-selling of improved services and tools (see Figure 4).
- > **Pay per use**—end users pay only for the services they use, and any costs associated with using the service, such as bandwidth. This differs significantly from the historical licensing model of selling software, which has dominated internet and IT business practice. User-pays models for the purchasing of computer services have opened opportunities, particularly for small-to-medium enterprises, to access cloud computing services that were previously only available to larger enterprises.

¹³ ACMA, [Communications report 2011–12](#), p. 4.

Figure 4 Revenue generation for Freemium cloud computing services



User data the new currency

Figure 4 highlights that, although free in name, there is an exchange of value, in terms of digital information, between end users and cloud service providers. In this type of supply chain, the end user is paying for the service by giving the provider access to their personal information. This can be done in several ways through:

> Advertising revenue

Paid advertising which is displayed while the service is being used. This method is common to online and social networking platforms. For example, Facebook has paid advertisements.

> Selling user data

This can come in two forms.

Cloud providers profile their users via personal data collected during provision of the service. This information can then be used to attract specific advertisers. The result is advertising that targets consumers' interests.

Alternatively the information can be anonymised and sold most often to data aggregators.¹⁴ Data aggregators sell this information to businesses and other parties seeking to learn more about their customers or to develop a better product for particular markets. For example, Facebook purchases information from data aggregators such as Datalogix to enrich consumer profiles.¹⁵

> Personalising the user experience

Services analyse the personal information of their users to enable them to better meet user needs and attract future users. Services such as Apple's iCloud make use of account holders' information in this way.

¹⁴ **anonymise** to carry out or organise in such a way as to preserve anonymity, *anonymised AIDS screening*, [Collins English Dictionary – Complete and Unabridged](#) © HarperCollins Publishers 1991, 1994, 1998, 2000, 2003 available at www.thefreedictionary.com/Anonymised.

¹⁵ OVUM, [Personal Data Futures: The Disrupted Ecosystem](#), 2013, p. 9.

This diversification of revenue streams, away from up-front payment, has potential benefits for end users including:

- > greater and more cost-effective access to desirable products and services
- > more individually tailored service experiences
- > the flexibility to ‘try’ services before making a financial commitment.

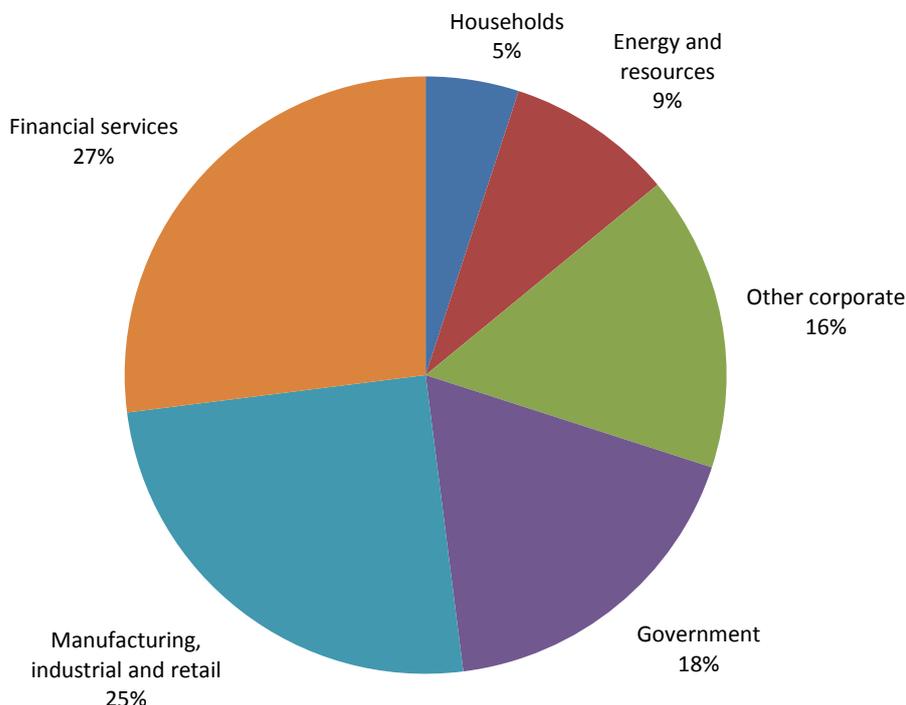
Changing revenue drivers for cloud computing have particular implications for users of these services. It raises issues for users about the sharing, control and ownership of digital information and particularly the privacy and security settings associated with personal information that is stored in the cloud.

Recent ACMA research into consumers’ use of location services identified that more than two-thirds of respondents were concerned about the level of information they shared. For the majority, the sale and ownership of information and the risks associated with disclosure were key concerns.¹⁶ Addressing these concerns will be important to enhancing user confidence for the wider adoption of cloud computing.

Connected consumers in the cloud

To date businesses and government are the primary users of private cloud computing services in Australia (see Figure 5).¹⁷

Figure 5 Australian cloud-computing industry, major market segmentation, June 2012



The significance of public cloud computing services is increasing in the Australian market as individual consumers increasingly create or store digital content as part of their daily lives, using a range of personal devices such as tablets and smartphones.¹⁸

¹⁶ ACMA, [Location services, personal information and identity: Exploratory community research](#), p. 49.

¹⁷ ACMA, [Communications Report 2—Australia’s progress in the digital economy: Participation, trust and confidence](#), 2012.

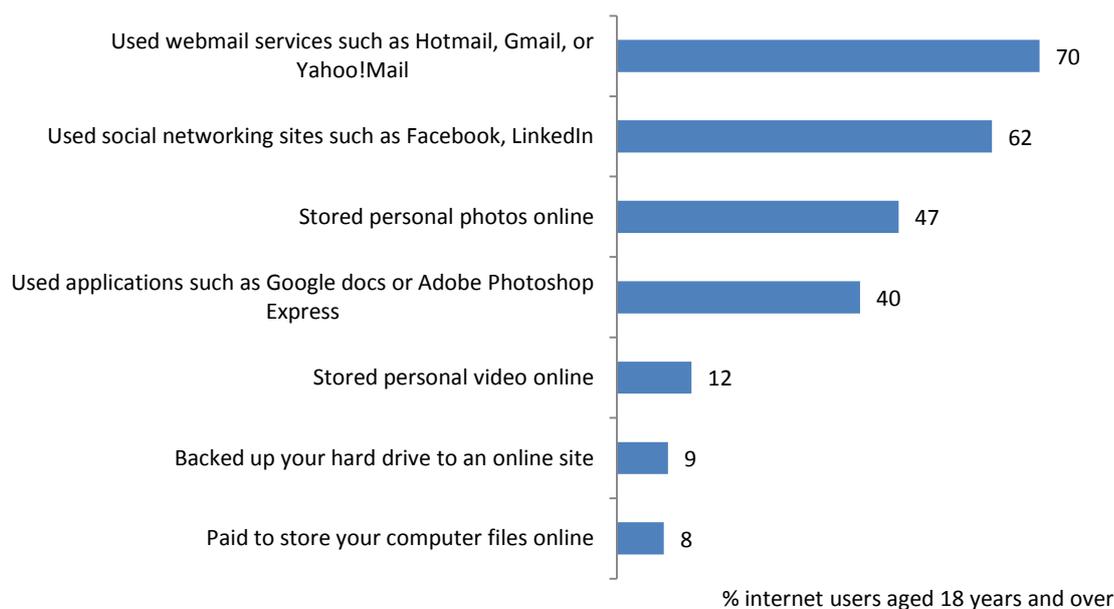
Cloud services also have the potential, through projects such as the [Global Public Inclusive Infrastructure \(GPII\)](#), to increase the functionality of access solutions for people with a disability to government and public services streamlining user preferences across services. This would:

- > reduce the costs associated with identifying, delivering and setting up accessibility interfaces for new services
- > simplify the use of new services through the provision of familiar interfaces and settings.

The popularity of smartphones has increased consumers' exposure to a range of cloud computing services, although Australian consumers still appear to be hesitant about using paid services. Previous ACMA research shows high use of cloud-enabled webmail, picture-sharing sites and social networking sites but only eight per cent paying to have data stored online.¹⁹ Products such as Evernote, Dropbox and Instagram have all built on this trend.

Figure 6 highlights the range of cloud computing services being used by Australians.

Figure 6 Use of cloud computing in the six months to May 2012



According to IDC research, 68 per cent of digital data in 2012 was created and consumed by individuals worldwide, with individuals generating 1,934 exabytes (EB) of data.²⁰ In an Australian context, the ABS estimates that during the 2012 June quarter, 421,147 terabytes (TB) of data were downloaded by Australian internet subscribers. This figure includes mobile downloads. And [IDC forecasts](#) that the cloud computing sector will be worth \$2,030 million by 2015, with estimates that by 2020 nearly 40 per cent of digital information will be 'touched' by cloud computing.²¹

¹⁸ ACMA, [Communications Report 3—Smartphones and tablets: Take-up and use in Australia](#), p. 33.

¹⁹ ACMA, [Communications Report 2—Australia's progress in the digital economy: Participation, trust and confidence](#), 2012.

²⁰ IDC EMC², [The Digital Universe in 2020: Big Data, Bigger Digital Shadows and Biggest Growth in the Far East](#).

²¹ *ibid.*

Consequently, the control and ownership customers have over their own content will become an increasingly important issue in the future as more of a user's personal data is stored beyond their computer. As part of this series, the ACMA will further explore this issue in a forthcoming paper on data protection and privacy.

Implications for regulatory settings

Similar to apps and near-field communications, cloud computing combines previously distinct elements of infrastructure, device, service and content in one product. Traditionally, these different elements of the communications delivery chain were regulated separately via service- or technology-specific regulation. As an example of a network-based service, cloud computing provides insights into pressures on regulatory mechanisms and settings that are straining to keep pace with contemporary communications.

The National Cloud Computing Strategy was released in May 2013. It outlines a vision for cloud computing in Australia that ‘... Australians will create and use world class cloud services to boost innovation and productivity across the digital economy.’²² The strategy identifies a number of actions to progress three goals:

- > the Australian Government will be a leader in the use of cloud services to achieve greater efficiency, generate greater value from ICT investment, deliver better services and support a more agile public sector
- > Australian small businesses, not-for-profit organisations and consumers will have the protections and tools they need to acquire cloud services with confidence
- > Australia will have a vibrant cloud sector supported by a skilled and cloud computing aware ICT workforce able to create as well as adopt cloud services, effective competition in cloud services and regulatory settings that support growth, foster innovation and protect users. The strategy recognises that promoting adequate consumer protection, clear information and fair dealings for consumers of cloud services will assist consumers acquire cloud services with confidence.

Actions identified in the National Cloud Computing Strategy include a proposed stocktake of regulation relevant to cloud computing. While the government has indicated there is no current need for cloud-specific regulation, there is currently a complex mix of industry standards, and international and national regulation, including economy-wide and industry-specific measures, relevant to cloud computing. A desirable outcome from the regulatory stocktake would be a streamlining of regulatory measures within a single coherent framework. The analysis of current regulation applicable in the cloud environment is an early contribution to a deeper analysis that may be undertaken as part of the planned regulatory stocktake.

This chapter discusses the current suite of regulatory measures that apply to cloud computing. It also covers current pressure points on regulation, including pressure to address identified areas of consumer and business concerns that may require different regulatory or non-regulatory solutions to boost confidence in the cloud environment.

Economy-wide and industry-specific regulation

Communications and media services have traditionally been regulated both at a national and international level.

Internationally, a range of organisations, such as the International Telecommunications Union (ITU) and the International Standards Organisation, provide technical and consumer standards. A range of development work is underway on standards and practices for data exchange and security protocols, which is discussed further in the chapter.

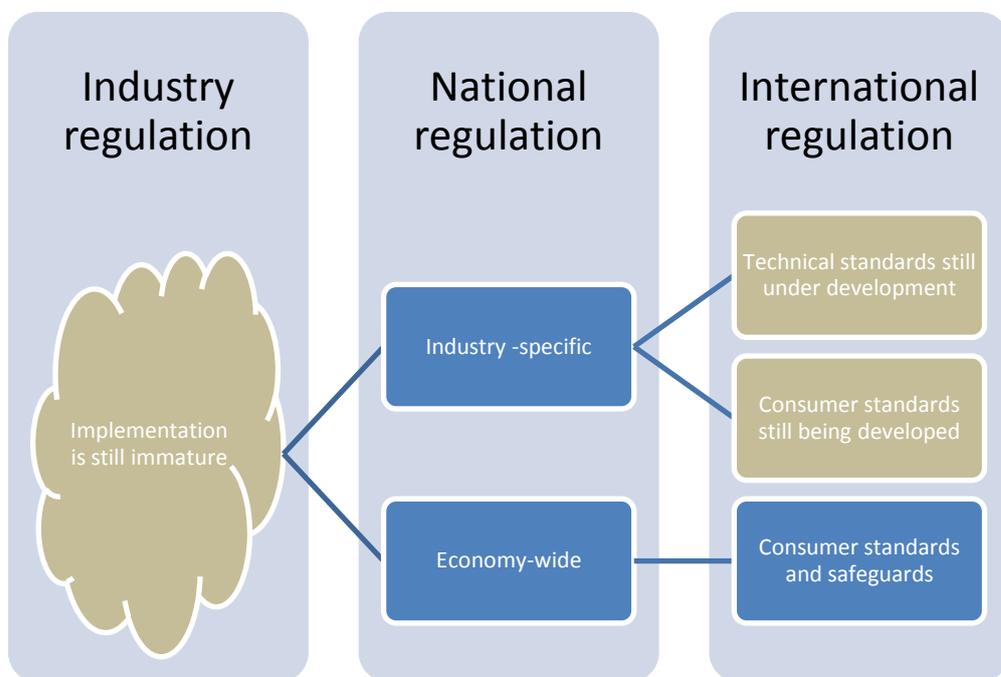
²² www.dbcde.gov.au/digital_economy/cloud_computing

At the national level, cloud computing is subject to economy-wide regulation that provides for basic consumer protections and safeguards. These include warranties against services which are not fit for purpose and false or misleading representation of products and services. Relevant whole-of-economy regulation applicable to cloud computing includes:

- > common contract law
- > Australian Consumer Law
- > the Privacy Act
- > the ePayments Code.

Figure 7 illustrates the regulatory environment in which cloud computing currently operates.

Figure 7 Australian cloud services regulatory environment



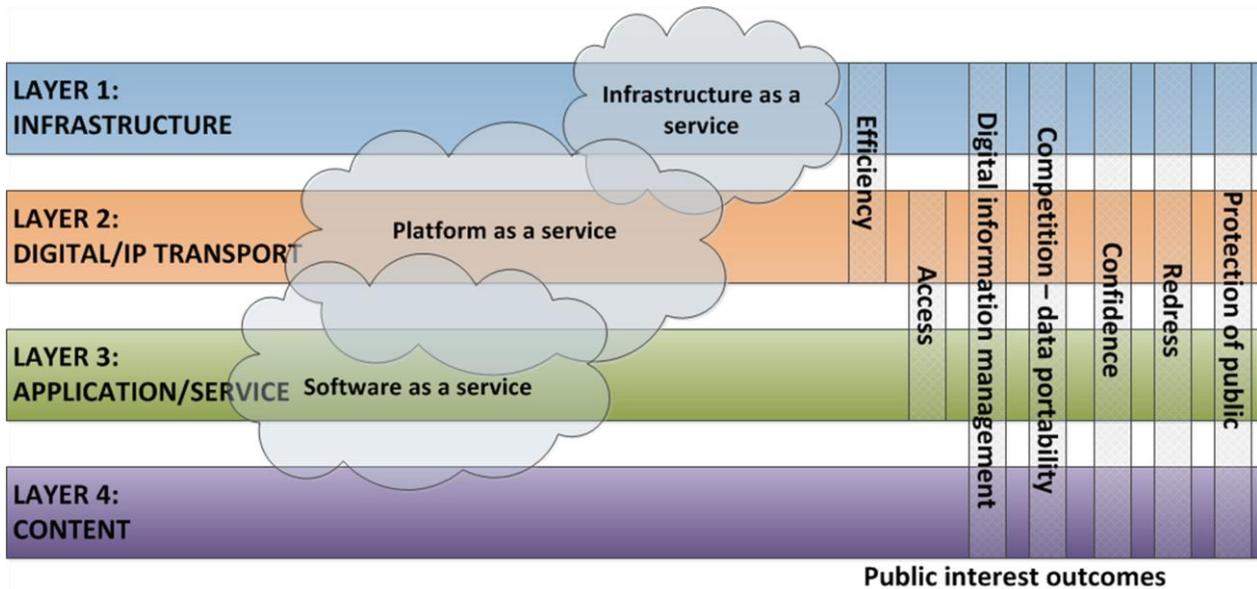
Cloud pressures communications regulation

Industry-specific regulation also applies to aspects of cloud service delivery at the national level. As the communications industry regulator, the ACMA's has sought to:

- > establish safeguards to protect consumers' interests, including complaints and redress mechanisms
- > provide safeguards to promote effective competition, such as being able to switch service providers and port services
- > ensure widespread access to networks and services;
- > manage public resources and establish rights of use to spectrum and telephone numbers.

These broad public interest outcomes remain relevant in the cloud environment, but existing mechanisms to achieve them are challenged by particular aspects of the cloud environment, including potential differential treatment of like services. Figure 8 illustrates the relationship between cloud computing and broad public interest outcomes.

Figure 8 Provision of public interest outcomes in the cloud



New industry participants challenge industry-specific safeguards

The developing nature of cloud services has brought many new service providers to the Australian market. Many are not traditional communications market players, as defined in existing legislation, such as internet providers, telecommunications companies or device manufacturers. Existing safeguards and information standards apply to particular industry participants or service delivery platforms. However, with new participants that do not align with existing legislative definitions, there is a risk that particular protections are not available to cloud users. There is also a risk that industry is uncertain about whether particular obligations apply or do not apply to their activities. An example of potential, differential regulatory treatment is that content-streaming and sharing services available on cloud computing may not be subject to the same obligations regarding classification information as television and radio that provide similar content.

As with other developing industries, new industry participants may not be familiar with existing regulatory obligations, such as consumer safeguards and protections. For example, this has implications for consumer safeguards around matters such as the privacy of personal communications, where data is stored in the cloud. When current privacy provisions were designed, developments such as cloud computing were not envisaged. There have been incremental adaptations of the regulatory framework to address the impact of technological and user behavioural change. However, this incremental approach is under pressure because of the scale and speed with which personal information can now be stored, exchanged and analysed, and made available to a wider number of market participants than those currently covered by communications privacy obligations.

Access to digital data just as important as access to networks

The ACMA has a role in ensuring competitiveness of the communications market, which it has often framed in terms of end users’ ability to switch between service providers. Currently, standards around portability and interoperability, which are common features of the communications and media environment, are still under development in the cloud computing environment.

At present, portability is framed within the context of number portability in Australian communications legislation.²³ The current focus of portability requirements is on telephone numbers and the services associated with those numbers. In the networked cloud environment, businesses and individuals are as concerned about maintaining access to their data and their online profile as they are about maintaining their telephone number. Data portability is the term used most often when referring to an individual's management of their digital information and is a mechanism for:

- > sharing data seamlessly between platforms, services and applications
- > transferring data easily between platforms, services and applications or from one to another.

Data portability, like number portability before it, has the potential to promote competition in communications and media because it would remove existing barriers in the cloud to end users' ability to easily change services.

Changing profile of demand for public resources

Cloud computing depends on reliable access to a broadband connection—fixed or wireless. Infrastructure development projects, such as the National Broadband Network, will address growing demand for high-speed broadband access. As importantly the growing emphasis by consumers on mobile devices and mobile services has also served as a driver for the adoption of cloud computing in Australia. In its role to plan and allocate spectrum, the impact of cloud service growth on future mobile broadband spectrum demands is an area of ongoing interest to the ACMA.

Addressing barriers to cloud adoption

In addition to addressing regulatory barriers to the development of cloud computing, current consumer concerns are another barrier to the take-up of cloud services.

Limited understanding about how cloud computing works and concerns about relevant protections for personal data use are current identifiable concerns. The main barriers to engagement with cloud computing can be categorised as:

- > security, privacy and the management of users' data
- > vendor lock-in, specifically concerns about interoperability and portability between cloud computing services, and loss of control of an individual's or a firm's data
- > data sovereignty—the ownership of data and access to data stored in countries, other than the one where the end user resides, including redress mechanisms.

Security, privacy and data protections

Cloud computing illustrates the growing level of interconnection between users and services. The amount and types of information stored, shared and analysed in the cloud are far greater than the name and address that was once available to the average telecommunications provider. As a result, the amount of information available to service providers is becoming increasingly detailed.

The majority of Australians have concerns about privacy online and 52 per cent lack confidence in privacy settings for online service providers.²⁴ More than two-thirds of Australians are concerned about the security and unauthorised use of personal

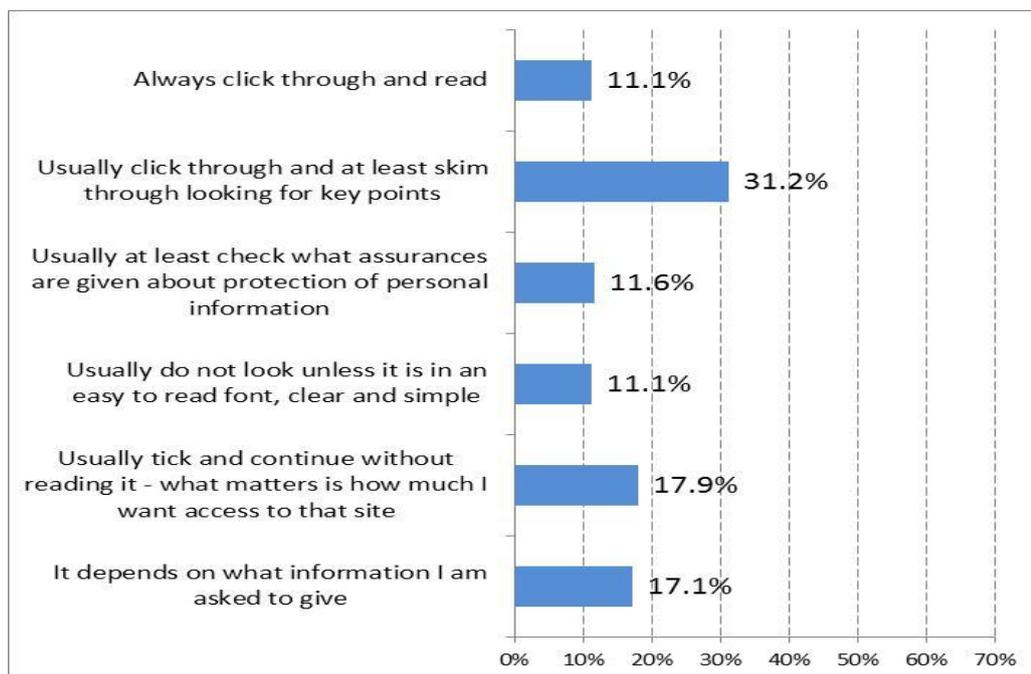
²³ [The Telecommunications Numbering Plan 1997](#) defines number portability as: '... the right of a **customer** receiving a service in relation to a number within particular number ranges to change either **the carriage service provider involved in providing the service**, the **carrier network involved in providing the service**, or both, and retain the same telephone number.'

²⁴ ACMA *Digital Footprints and Digital Identities- Community research, 2013* (unpublished)

information by providers.²⁵ Recent ACMA community research shows high consumer use of cloud-enabled webmail, picture-sharing sites and social networking sites. However, only eight per cent are paying to have data stored online, suggesting that they are taking explicit decisions to limit their cloud activity.²⁶

Research into location services by the ACMA showed that consumers expect to be informed by their service providers about the terms of use of their personal information.²⁷ At the same time, as Figure 9 illustrates, two-thirds of Australians choose not to read or only occasionally read terms and conditions before accepting the terms of use of digital services and applications.²⁸

Figure 9 Attention given terms and conditions of use



Cloud computing, particularly public cloud computing services, which are currently most used by individuals, often have proprietary standards and service agreements, which may impact on an individual's ability to manage their information. For example, the current terms and conditions for use of webmail services often allow for the anonymous collection of personal information. Users of these services have little graduated control or visibility of information collection and sharing practices under the terms and conditions of service. There is evidence of the tension between consumers' expectations and behaviour, and the current models establishing service terms and conditions. This can be seen in the ongoing disagreements between Facebook and its users over privacy settings and other account settings, and the outrage of users of [Instagram](#) in its proposed change in terms of use.

Growing concerns about privacy and the management of personal information are apparent internationally, with regulatory and non-regulatory approaches to dealing with these issues being developed in markets such as the US and the European Union (EU). For example, the US has been working for some time on a 'Do not track' option for web browsers, which has seen limited voluntary adoption.

²⁵ ACMA, [Communications Report 2—Australia's progress in the digital economy: Participation, trust and confidence](#), 2012, p. 25.

²⁶ *ibid.*, p. 17.

²⁷ ACMA, [Here, there and everywhere—Consumer behaviour and location services](#), 2102, pp. 20–21.

²⁸ ACMA *Digital Footprints and Digital Identities- Community research, 2013* (unpublished)

The EU has recently completed a full review of its Privacy Directive.

Vendor lock-in, portability and ease of switching providers

A common feature of public cloud computing services, such as webmail, content sharing and storage, is the use of proprietary standards and service agreements. Proprietary standards may limit a business or an individual's ability to easily transfer their data, or may prevent them accessing their content via other services. Email is a very common cloud service and a customer can migrate to a new provider and a new address. In this case, the customer or the customer's correspondents may be aware of the implications of different data requirements such as addresses, earlier emails and attachments. There are degrees of difficulty with other types of cloud computing services. For example, a consumer who has stored their music collection in one cloud service may be unable to easily transfer the entire collection to another. This can be because they do not have a copy of the music files on their own computer or device, or the files are in a proprietary technical standard that is incompatible with those used elsewhere.

Currently, there is no open standard or technical specification that ensures data portability between data controllers.²⁹ Data portability is a prerequisite for users of cloud computing services, if they are to have an ongoing choice between providers for a range of services, but the challenge of providing data portability is different with each cloud service type. There are efforts underway, such as [open source software tools](#) that facilitate exportation of data and [non-for-profit organisation advocating data portability](#). At a supra-national level, the EU is considering a proposal for regulation of personal information, [including a right to data portability](#).

At present, the lack of interoperable technical standards between cloud computing services means that users may risk losing their content and media if they change services. For both business and consumers, this is an increasingly high barrier as social and professional lives move online.

Data sovereignty and redress

Cloud computing service providers are often based internationally and national economy-wide legislation, such as privacy, may not capture providers based in other jurisdictions. Cloud providers based in international jurisdictions may be subject to local legislation and this has raised concerns about end users' ability to manage access to their personal information in accordance with the protections available in their home country.³⁰ Recent ACMA consumer research identified that 35 per cent of Australians would withhold personal information if the site was not based in Australia.³¹ This issue has been referred to as data sovereignty, and illustrates the difficulties for users in a globalised market of being able to take action or seek redress against cloud providers in other jurisdictions. One response to this practice has been for some cloud providers to establish data centres in Australia. The low numbers of Australian-based data centres, particularly among public cloud providers, has been identified as an issue for consumers and business concerned about the security and ownership of their data when stored in other jurisdictions.³² Some of the larger international cloud providers such as Google, IBM and Amazon, have begun to address the data sovereignty concerns of users by providing the option for the end

²⁹ [Nokia Position on the European Commissions' consultation on proposed reforms to the European Data Protection Framework](#)

³⁰ KPMG, [Modelling the Economic Impact of Cloud Computing](#), p. 11; ATSE, [Cloud Computing: opportunities and challenges for Australia](#), p. 9; Michael Lee, [What Australian businesses need to know about cloud compliance](#), ZDNet, March 2013.

³¹ ACMA *Digital Footprints and Digital Identities- Community research, 2013* (unpublished)

³² KPMG, [Cloud computing: Australian lessons and experiences](#), p. 14.

user to choose the jurisdiction their data is stored in and moving to build data centres in Australia.³³

In an information economy, the efficient management of digital data has potential productivity benefits. The current fragmented nature of regulatory arrangements that apply to cloud computing services, including international approaches under development, creates complexity for would-be cloud computing service providers and for individuals choosing to use cloud computing services for their digital data.

A useful outcome of the planned stocktake of regulation relevant to cloud computing would be a streamlining of activity within a single coherent regulatory framework.

³³ Brad Howarth, [‘Bring it on: locals ready to fight as the global giants muscle in’](#), *The Australian*, April 2013.

Regulatory strategies for confidence in the cloud

Strong commercial, economic and social benefits stem from the free flow of information. Balanced against these benefits are social and business interests concerned with the protection of commercial and personal digital data. Getting the balance right will be important in addressing current barriers to the adoption of cloud computing that are apparent in the Australian market, and improving overall confidence in cloud computing services. This is likely to require a multi-layered approach that addresses:

- > confidence in overarching global governance structures that support digital data in the cloud
- > initiatives by Australian industry participants
- > working with business and consumers to provide them with the skills and knowledge to assist them in positively managing their digital data in the cloud environment.

Confidence in standards and global governance for digital data

As cloud computing services support global flows of digital data, and with many of the larger cloud providers operating internationally, any action to address current barriers to service adoption will need to incorporate a multi-jurisdictional dimension.

Current initiatives focus on developing a more certain, stable environment for cloud computing based on:

- > industry standardisation efforts
- > government endeavours to address transparency of data management and security practices for business and individuals.

Many international standard-setting bodies are examining possible solutions for intermediating between cloud operations, and between users and cloud providers.³⁴ Standard development activity is ongoing, within the [International Telecommunications Union](#) (ITU) and the [Internet Engineering Task Force](#) (IETF) with efforts directed to the specification of functions and protocols that allow data exchange between cloud computing services. This same issue is also being addressed by national or regional entities such as the US-based [National Institute of Standards and Technology](#) (NIST). The government also seems to have recognised the importance of standards in the National Cloud Computing Strategy and has committed to strengthen engagement with regional and international standards and technical committees, and is also committed to encourage involvement in the private sector.

Transparent data management, privacy, and security practices are a focus for government regulatory efforts such as the [European Union Data Protection](#) Directive. With data protection frameworks under review in many jurisdictions, the response in other jurisdictions has been directed to the development of industry self-regulatory responses. [The New Zealand Cloud Computing Code of Practice](#) and projects such as the [Cloud Security Alliances' Trust and Assurance Registry](#) address data sovereignty concerns by ensuring end users are informed about and are aware of the implications

³⁴ For a survey of the SDOs (Standard Development Organisations) involved and their activities see Cloud-0-0084R1, a report to the ITU Focus Group Cloud for a meeting in Geneva, December 2011.

of the relevant privacy, security and information-sharing rules of the jurisdiction their data is stored in. In the Australian context, initiatives include:

- > the [Australian Government Information Management Office \(AGIMO\) guidance on government engagement with cloud services](#), as part of the National Cloud Computing Strategy
- > the development of a voluntary Cloud Consumer Protocol aimed at encouraging information disclosure by cloud service providers and supporting consumers of cloud services in being well informed. The ACMA understands that the Australian Computer Society is responsible for developing the protocol and will be conducting national public consultation with the aim of having the protocol in place by the end of 2013.

The global nature of the cloud industry, and the diverse range of cloud computing service providers, will inevitably challenge efforts to directly regulate all components of cloud services. As these examples demonstrate, there are different models under development at national and international levels, with associated cost increases for cloud providers in meeting different standards and compliance approaches.

In such an innovative environment, it is more likely that collaborative efforts by regulators and industry participants, directed to harmonisation of treatment between countries, will be an important strategy in providing more stable arrangements for global cloud providers. Such cross-border strategies are also likely to adopt a range of interrelated tools, including regulation, education programs for consumers and industry, and technology-based approaches such as technical standards development. The ACMA's experience with other global communications issues, such as unsolicited communications, indicates that a multifaceted approach can yield positive results for industry and consumers in managing digital data across national borders.

Facilitating industry cloud initiatives

Industry-led initiatives, to address known barriers to service take-up, have the advantage of allowing more flexible responses to issues in an emerging market such as cloud computing. A number of cloud computing services have differentiated their offerings based on providing Australian-based data centres³⁵, or increased end-user control of security, such as through encryption before data is uploaded.³⁶

Although there have been attempts to encourage the development of an industry self-regulatory approach, such as the [Australian Consumers Action Network \(ACCAN\) guide for cloud providers on consumer protection principles](#), the cloud industry in Australia has yet to develop a code of conduct. In part this may be a reflection of the diverse nature of the participants and the small number of cloud providers with data centres based in Australia at present.

From the ACMA's past experience in industry co and self-regulatory schemes, a common industry interest is one of the markers for successful self-regulatory solutions, along with a competitive market, few barriers to entry and a rapidly changing environment.³⁷

Many of the conditions for effective self-regulatory responses are present in the cloud market in Australia. As barriers to the adoption of cloud services become more pressing in Australia, it is likely that there will be a more compelling case for industry-led responses to industry standards and data protection and security.

³⁵ Brad Howarth, 'Bring it on: locals ready to fight as the global giants muscle in', *The Australian*, April 2013.

³⁶ For example [wuala](#) promotes user control of encryption as part of its service.

³⁷ ACMA, [Optimal conditions for effective self- and co-regulation, Occasional paper](#), 2011.

Confident consumers

Communication strategies offer a flexible response to addressing emerging issues in digital communications and information, where improvement in knowledge or industry or consumer behaviour is the intended outcome.

There are opportunities to address known areas of consumer concern about the sharing, control and ownership of digital information in the cloud through the provision of information on how they can manage their data privacy and security settings. Importantly, an individual's ability to effectively manage these services also depends largely on their own understanding and their ability to take action—their digital literacy.

Addressing differences between user expectations for informed consent, and their behaviour in providing electronic acceptance of terms and conditions, may also require cooperative action by regulators and cloud providers. The aim would be to improve users' awareness of any implications for the storage, collection, analysis and use of their digital information in the cloud environment. The ACMA's community awareness and information programs, dealing with other forms of digital information practices in [anti-spam](#) and [cybersafety](#), are models for improving consumer skills and confidence in the cloud environment.

Conclusion

Cloud computing, while not a new idea, is rising in prominence. In part, this is due to the growing success of the apps market and the ongoing demand by consumers and business for access to their content and media anywhere and on any device. The cloud industry is diverse and globalised. It illustrates many of the concerns being expressed by consumers around the privacy, security and management of their personal information in a globalised information economy.

Cloud computing represents a range of communications services, which are moving beyond traditional business models and capitalising on changing consumer behaviour. Consumers are sharing digital information in online environments at an unprecedented level. However, some are concerned about the transparency of data management and the privacy practices of cloud service providers, which inhibits their take-up and engagement with cloud computing.

Strengthening consumer confidence in the use of cloud computing is likely to require further action from both industry and governments. Such action would address global governance arrangements for cloud computing, the ease of switching cloud providers and transferring data, along with assurances about relevant protections for personal information in an information economy.

Cloud computing is currently subject to a mix of economy-wide and industry-specific regulatory measures, as well as emerging international standardisation efforts. Reducing regulatory complexity, while also balancing business and consumer concerns about personal data protections, is an early area for action that would underpin a more stable and confident environment for cloud computing.

A stocktake of regulation is an important first step, but other initiatives to promote confidence in cloud computing would benefit from sound underpinning within a single, coherent regulatory framework. This should help establish strong foundations for cloud computing in Australia and realise productivity benefits for business, while balancing important business and consumer concerns. Given the potential economic and social benefits offered by cloud services, there is merit in having cloud issues considered within a single coherent regulatory framework.