Demystifying Personal Cloud Services

An investigation of Australian consumer expectations and experience

RMIT UNIVERSITY

accan

Demystifying Personal Cloud Services

An investigation of Australian consumer expectations and experience

Alemayehu Molla, Vanessa Cooper, Ahmad Abareshi, Siddhi Pittayachawan

July 2015

RMIT UNIVERSITY

accan

Demystifying Personal Cloud Services: An investigation of Australian consumer expectations and experience

Authored by A. Molla, V. Cooper, A. Abareshi and S. Pittayachawan

Published in 2015

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

RMIT University
Website: http://www.rmit.edu.au/
Email: alemayehu.molla@rmit.edu.au

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000
TTY: 02 9281 5322

ISBN: 978-1-921974-31-1
Cover image: iStockphoto © 2013

This work is copyright, licensed under the Creative Commons Attribution 3.0 Australia Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the authors and "RMIT, supported by a grant from the Australian Communications Consumer Action Network". To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/au/

This work can be cited as: Molla, A, Cooper, V, Abareshi, A & Pittayachawan, S 2015 *Demystifying Personal Cloud Services: An investigation of Australian consumer expectations and experience*, Australian Communications Consumer Action Network, Sydney.

Acknowledgements

The project team would like to acknowledge the contribution of many people throughout this project.

Thank you to all of the participants in our study who gave their valuable time and insights during our interviews, focus groups and survey. Without this input, the project simply would not have been possible.

Special thanks also to the Australian Communications Consumer Action Network (ACCAN) team, particularly Narelle Clark and Katerina Pavlidis, who provided invaluable guidance and feedback throughout each and every stage of the project.

We thank our colleagues from RMIT University who have supported us in completing this project. In particular, we would like to thank Angeline Bartholomeusz from the College of Business' Research Office for her support in developing the project proposal and Emeritus Professor Margaret Jackson from the Graduate School of Business and Law for her feedback on the review of relevant legislation. We also thank our colleagues in the School of Business IT and Logistics Finance Team, College of Business Research Office, RMIT Post-Award Services and RMIT Communications for their various assistances.

Finally, we wish to thank ACCAN for the grant that made this project possible.

Executive Summary

This project was undertaken to study Australian individual consumers' use of personal cloud services. The aims were to identify consumers' personal cloud awareness, behaviours, experiences and expectations, and to develop recommendations and guidelines that address the issues and challenges that confront consumers and that improve the quality of their experience.

The United States (US) National Institute for Standards and Technology (NIST) has defined cloud computing as 'a model for ubiquitous, enabling 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' (Mell & Grance 2011:p2). The personal cloud is a transformational model of cloud computing in the individual consumer domain. Gillett et al. (2011: p.6) define personal cloud as 'a set of personal devices and federated online services configured and controlled by individuals that 1) organises and preserves personal or work information, documents, media, and communications; 2) delivers that information to any device or service; and 3) orchestrates integration of personal information across digital devices and online services'. There are many personal cloud models. Nonetheless, this project has primarily focused on four types of personal cloud services and excluded email, social media, online television and other cloud-based online services. The four services are:

- Software as a service: online software programs deployed in a public cloud that consumers use based on subscription without the need to download or install them on their computers. Examples include Google Docs, Google Sheets and Evernote.
- Storage as a service**:** an online space provided to the public, usually through a freemium pricing model, to store, back up and share digital content. Although some of the software as a service models incorporate storage as a service, not all storage as a service models offer software. Examples include T-Cloud, Google Drive, Dropbox, SkyDrive, OneDrive, Amazon Cloud Drive, Box and JustCloud.
- Backup as a service: a service to back up digital content and devices. Examples include iCloud, iDrive and OpenDrive.
- Computing as a service: computing services that recreate a personalised setting of a consumer's desktop with an online version accessible from anywhere through the internet. Examples are Amazon and GoPC.

The project involved interviews, focus group discussions, surveys of self-reported users (479) and non-users (474) of the personal cloud and desk research. The key findings were:

- Not all the consumers fully understood how personal clouds work, what they offer, and what they mean for data security and privacy. In some cases, the consumers did not consciously choose to use a cloud service; instead, the service was attached to their device, leading to an unintentional form of cloud use. Indeed, 85% of the 479 consumers that used the personal cloud did so without, or with very little, understanding of how service providers use their data or metadata, or the risks involved and the precautions to be taken in using a cloud service.

- Among the 479 consumers that reportedly used the personal cloud, more than 80% used cloud storage and backup services and two-thirds used cloud software to create and manage digital content. One in two consumers (ranging from 12% of over 55s to 50% of 18–35 year olds) used a do-it-yourself private personal cloud, either on its own or in addition to a public personal cloud. Although Australian consumers use a range of personal cloud services and providers, they tend to stick with well-known global brands rather than local Australian companies. Apple, Dropbox, Google and Microsoft make up 86% of the personal cloud services reported in the survey and interviews. Whether consumers lived in urban, rural or regional areas, their residency did not significantly affect their choice of personal cloud model.
- The majority (88%) of the 479 users who completed the user survey did not pay for cloud services and were content to stay within the free limits given by providers. Those that were paying spent on the average $222 per year. In addition, only 12% of all the 953 survey participants intended to pay for a personal cloud service within one year. For one out of five consumers, their use of the personal cloud, rather than reducing their information technology (IT) expenditure, had resulted in an increase in their IT expenditure due to acquiring new devices and upgrading data plans. However, consumers are becoming increasingly savvy in ways to prevent bill shock due to the cloud. In the past two years prior to the survey, only 23% of users had had to pay excess fees at least once because they exceeded the free allowance or paid subscription limits of the personal cloud. Younger and male consumers were more likely than older and female consumers to incur excess fees.
- Users and non-users of the personal cloud significantly differed in terms of their motivation. For users, mobility to access and share their digital content easily from anywhere, anytime and any device were what primarily motivated them to use the cloud, followed by overcoming storage and mobile device limitations. However, 65% of the 474 non-users either did not have a need or were uncertain if they needed the personal cloud. One in three users faced workplace expectation to use the personal cloud. Yet only one in five of the non-users would use the cloud if it became a workplace requirement.
- Two-thirds of those living in regional and rural communities and half of those in remote communities were using the personal cloud because of a need to access files across different devices, whereas two-thirds of urban dwellers were motivated to access files from different locations.
- The current rhetoric about the personal cloud is hardly positive. There is a widespread fear that extensive use of the personal cloud makes the level of surveillance that would have been illegal in the physical world possible in the electronic world. Nevertheless, not all the consumers thoroughly read the terms and conditions of contracts to realise the geolocation of a cloud server or the applicable legal jurisdiction. Further, most consumers did not always take basic personal precautions on the cloud and the majority rarely planned for digital inheritance.
- Key consumer issues around the personal cloud include privacy, security and data sovereignty. There was understanding by the consumers that their data were valuable to companies; however, they did not necessarily understand the extent of that value. Only a few emerging cloud models (such as Meeco) are considering passing this value back to consumers.

- Only 18% of all the consumers surveyed believed that there are adequate regulations for personal cloud services. Nevertheless, in our assessment of telecommunications consumer-related laws and codes, we did not find any particular regulation or legislation that was a real barrier to personal cloud services flourishing in Australia. The existing regulations and tools, although they are not specific to the personal cloud, are broad and flexible enough to cover most of the known consumer concerns. Nevertheless, some grey areas, such as data breach liability and notification, cloud service levels, interoperability of services and copyright exceptions covering fair dealing, format and time shifting, create uncertainties.

Recommendations for Consumers

Assess personal cloud readiness. The personal cloud requires a high-bandwidth internet connection with a decent data plan. This creates a high degree of dependency on the network, and consumers may be locked out of their digital content through network disruptions. Consumers must evaluate the extent of their digital content, their demand for data upload or download, their mobility, and the quality and affordability of the internet connection available to them in order to choose a personal cloud service that best maximises their experience. If consumers do not have a high-bandwidth connection, data transfer will be sluggish and the cloud experience unappealing.

Caveat emptor. Consumers should consider their current and future needs for a personal cloud in choosing digital devices (e.g. mobile phones, tablets and computers) as, increasingly, cloud services are attached to their devices and result in an 'unintentional choice' of cloud providers. Australian consumers have a range of cloud services and providers from which to choose, and they should weigh up the advantages and disadvantages offered by large well-known global brands versus small local Australian companies offering niche services.

Avoid click-through behaviour. Personal clouds are provided under standard contracts, which are regulated under the Australian Consumer Law (ACL). These contracts allow service providers to change the performance of their cloud services, such as in size, speed and file delivery mechanisms, without consumers' consent. Consumers need to avoid the 'click-through behaviour' whereby they do not read the terms and simply click the 'agree' button to complete the registration process without awareness of what is written in the terms. The consumer guide included in this report can assist to mitigate this issue by identifying the most common areas that consumers need to scrutinise in service contracts.

Apply personal precaution. Data security and privacy both during transmission and on the cloud are major concerns for most consumers. Despite consumers' expectations of reassurance from regulatory agencies as well as service providers that their data are in safe hands, most consumers are not taking personal precautions to secure their personal cloud use. These personal precautions include managing usage to avoid excess fees, checking the terms of service to ensure that their cloud provider has a third party (such as TRUSTe) certification or complies with known data-handling standards such as the US-EU-Switzerland Safe Harbor Framework, setting a strong password for tablets, mobiles and personal computers, activating the security features of cloud services, being selective about what digital data to keep in the personal cloud and keeping backup.

Plan for digital inheritance. The personal cloud increases consumers' digital content and elevates the need for planning who can access their online accounts after their death. The issues include who will inherit data, how to authenticate multiple accounts, how to respect the privacy of the dead and their correspondents, how to dispose of the digital footprint and who will own digital credentials. Consumers need to have an appropriate plan in their will for how their digital assets will be passed on after their death.

Recommendations for Personal Cloud Providers

Full service disclosure. The personal cloud space is emerging. Considering that some consumers do not have a full understanding of what they are using, what they are signing up for, where data end up, and their rights and obligations, there is an issue of the extent to which providers are providing a full product disclosure that satisfies existing laws in a form that is accessible to a wide range of consumers.

Cater for digital footprint and inheritance. When consumers can no longer use a service for reasons such as death, the way in which providers handle the consumers' data is not entirely clear. The issues include who will inherit data, how to authenticate multiple accounts, how to respect the privacy of the dead and their correspondents, how to dispose of the digital footprint and who will own the digital credentials. Whereas some service providers do not specify a clear policy addressing these issues, others have clauses that restrict the 'right of survivorship and non-transferability'.

Improve quality of experience. Consumers are experiencing a number of inconveniences with personal clouds such as inconsistency in multi-device file synchronisation, unfriendly user interface, slow speed in uploading and downloading files, and delay in starting cloud applications. As a result, less than 50% of consumers consider personal clouds to be reliable, trustworthy and meeting their service level expectations. The fulfilment of consumer expectations encourages wider cloud uptake. If performance levels do not reach expectations because quality is compromised too much, consumers will reject the service or refuse adoption. Providers should thus pay more attention to the user experience.

Include minimum service levels in standard contracts. Although some cloud service providers undertake to make necessary backups, only one of the providers that we investigated warranted data integrity, or accepted liability for data loss. Minimum service level standards would make it easier for consumers to compare different services. Further, in addition to providing their detailed terms and conditions, cloud providers might 'translate' their detailed terms and conditions to provide consumers with an abridged version that provides less 'legal speak' but is more likely to be read and understood by average consumers.

Work to establish standards for interoperability. Portability is the key to competition in cloud services. Personal cloud services are not fully interoperable, which creates some difficulty (inconvenience) in moving data across different service platforms. The industry has to work on voluntary interoperability standards. The lack of interoperability can lead to consumer lock-in by making switching from one service to another impossible, too costly or unattractive.

Recommendations for Regulatory and Consumer Agencies

Consider mandatory data breach notification in future law reforms. The *Privacy Act 1988* and its accompanying Australian Privacy Principles regulate the handling of personal data. Nevertheless, the Act currently does not specify the obligation of personal cloud service providers to inform consumers in case of a data breach. Future law reforms need to consider mandatory data breach notification.

Monitor to ensure that free personal cloud services have the same consumer protection standards as paid services. Personal cloud providers do not provide warranties as to the availability and performance of cloud services. This means consumers could be subject to data loss if a service provider discontinues (or disrupts) its services for various reasons. However, the Australian Consumer Law stipulates consumer guarantees that cannot be excluded by service contracts. There is potentially a variation between the service providers' terms and applicable Australian laws whereby contract terms may limit the liability of a guarantee. Further, personal cloud contracts favour service providers since they can change the performance of the cloud services, such as in size, speed and file delivery mechanisms, without consumers' consent. This is one area that needs to be examined more closely to ensure that personal cloud contracts are consistent with the ACL. The issue is further complicated by the fact that most consumers use personal cloud services provided by international companies and there may be practical challenges in enforcing the relevant Australian laws when the provider is based overseas**.**

Prioritise the enforcement of the Australian Consumer Law on major international personal cloud providers. Government agencies such as the Australian Competition and Consumer Commission (ACCC) might further prioritise enforcement of the ACL by international personal cloud service providers. In the meantime, educate **consumers** so that they are well informed about cloud products and services as well as the practical challenges of enforcing the ACL on overseas personal cloud providers. Consumers use cloud services from both Australian and overseas providers. There is a need for clarity as to which Australian regulations apply and the extent of protection or regulation that they afford to personal cloud consumers that use overseas providers. Although the ACL will ordinarily apply, there may be practical challenges in enforcing that regulation, for example, if the provider is located overseas.

Implement a protocol for cloud computing to encourage information disclosure by cloud providers and support consumers of cloud services in being well informed. The Australian Computer Society (ACS) in consultation with the Australian government initiated a discussion paper on a national cloud computing protocol (NCCP). At the time of the consultation, in 2013, there was a lack of support for an NCCP from major cloud vendors, industry bodies and telecommunications providers. These stakeholders considered that the protocol would replicate existing regulatory protections and complaints mechanisms that were already deemed effective. However, we believe that a national protocol can provide a consistent approach to cloud service providers to be upfront with consumers in response to data privacy and security issues and facilitate the integration of cloud services with extant Australian consumer protection and privacy laws.

Ensure that the personal information collected by personal cloud providers (particularly overseas personal cloud providers) meets the definition of personal information under the *Privacy Act 1988* and the method of data collection and their use comply with the Australian Privacy Principles.

Reassure consumers that are concerned about personal cloud–related digital surveillance that unless a warrant is issued, existing regulations provide sufficient protection to the confidentiality of consumers' data during transmission and storage. Consumers need to be educated that it is easy to intercept data transmitted across unencrypted wi-fi networks.

Establish (or clarify) the mechanism for addressing personal cloud disputes. Unless a personal cloud service is provided by a carriage service provider, it is unlikely that the Telecommunications Industry Ombudsman (TIO) (which focuses on the supply of landline, mobile and internet communications) can provide dispute resolution services to personal cloud consumers. It is also important to explore whether the Telecommunications Consumer Protections (TCP) Code provides adequate coverage to the privacy, billing, customer transfer and complaint-handling issues of personal cloud services.

Table of Contents

Acknowledgements i

Executive Summary iii

Table of Contents ix

INTRODUCTION 1

LITERATURE REVIEW 3

Diffusion of the Personal Cloud 3

Benefits of the Personal Cloud 3

Factors that Influence Personal Cloud Adoption 5

Individual factors 5

Vendor-related factors 5

Institutional factors 6

Cross-cutting issues 7

METHODOLOGY 8

Interviews 8

Focus Group Discussions 8

Q-Method Interview 8

Survey 9

Desk Research 11

FINDINGS AND DISCUSSION 12

A Taxonomy of Personal Cloud Services 12

Consumers' Awareness of the Personal Cloud 14

Personal Cloud Use 16

Premium v. 'Freemium' Cloud Consumers 20

Motivation for Using a Personal Cloud 21

Consumers' Fears and Doubts 22

Personal Cloud Self-Efficacy 24

Criteria for Choosing a Personal Cloud 27

Personal Cloud Precautions 27

Personal Cloud Quality of Experience 28

Personal Cloud and Communications Consumption 29
Future Intentions 31
Most and Least Important Personal Cloud Issues 32
Most important issues 35
Least important issues 35
Evaluation of Consumer Protection and Privacy Codes 36
Main regulatory instruments for personal cloud services 36
Geolocation 37
Personal cloud security 37
Privacy of data in personal clouds 37
Data retention 38
Premium pricing 38
Interoperability 38
Copyright 39
Terms of service 39
Service warranties 39
Consumer complaints and dispute resolution 40
CONCLUSIONS 41
The Personal Cloud is Not Truly Personal in Its Current Form 41
To Cloud or Not to Cloud 41
Consolidation of the Personal Cloud Market 41
Data Value Asymmetry 42
One Size Does Not Fit All 42
Risk averters 42
Productivity maximisers 42
Social users 43
Cloud hesitators 43
Vault seekers 44
Cloud usability explorers 44
The Regulatory Environment for the Personal Cloud 44
RECOMMENDATIONS 46
Recommendations for Consumers 46
Recommendations for Personal Cloud Providers 47

Recommendations for Regulatory and Consumer Agencies 47
Authors 50
Glossary 51
Figures and Tables 52
Figures 52
Tables 52
APPENDICES 53
Appendix A: Profile of Interview and Focus Group Participants 53
Appendix B: Detailed Profile of Q-Interviewees 55
Appendix C: Q-interview Sorting Scale 57
Appendix D: Sample of a Completed Q-interview Sheet 58
Appendix E: Six Distinct Groups of Personal Cloud Consumers 59
Appendix F: Correlation among the Six Groups 59
Appendix G: Crib Sheet 60
References 62
Legislation 66

INTRODUCTION

This project was undertaken to study Australian individual consumers' use of personal cloud services. The United States (US) National Institute for Standards and Technology (NIST) has defined cloud computing as 'a model for enabling 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' (Mell & Grance 2011:p2). It is a form of distributed computing, developed from the characteristics of both cluster and grid models in which a third party owns the technical infrastructure and delivers services to end users (Qiong, Liu & Pang 2013). Cloud computing is a rapidly growing area and has expanded into an estimated $46 billion market, representing around 17% of global software sales (Teneyuca 2011).

The personal cloud is a transformational model of cloud computing in an individual consumer domain. The Australian Communications and Media Authority (ACMA 2014) estimated that 71% of Australians use a form of cloud service, often without realising that they are doing so. Therefore, there is still some degree of confusion as to what the personal cloud is. For example, Andersen and Karlsen (2011) defined the personal cloud as anything consumers can access on the cloud infrastructure, including private information to which others have no access, as well as information shared between individuals such as co-workers or friends. Ernst (2012) argued that, in order for a cloud to be truly personal, the owner of the personal cloud must be able to:

> choose and remove the apps they run on their personal cloud … control who does and does not get access to the data … process data created with one app with another in a similar way as files on a PC may be opened by apps from a different vendor … set the terms of use themselves move the personal cloud from one host / infrastructure / hosting provider to another if needed.

There are hardly any services that satisfy these stringent conditions.

Therefore, a working definition of personal cloud is:

> a set of personal devices and federated online services configured and controlled by individuals that 1) organises and preserves personal or work information, documents, media, and communications; 2) delivers that information to any device or service; and 3) orchestrates integration of personal information across digital devices and online services. (Gillett et al. 2011: p.6)

The use of a personal cloud requires a certain degree of skill and knowledge. Consumers' confidence in, and judgement of, their ability to choose and use a cloud service effectively can influence their experience. Some users are unaware of audit rights on their own data or on the personal cloud service provider, and this must be understood before agreeing to the contract. Nevertheless, personal clouds are provided for under 'standard contracts'. This creates 'click-through' behaviour, whereby consumers do not read the terms and simply click the 'agree' button to complete the registration process; as a result, the majority of consumers may not be aware of what is written in the terms. There is also a lack of evidence on how the personal cloud is affecting consumers'

communications consumption, their digital lives, experiences and expectations, and the issues surrounding these. It is also important to identify the pitfalls and risks of using a personal cloud as well as the existing consumer protection measures.

Therefore, the aims of this study were to define personal cloud services; identify consumers' personal cloud awareness, behaviours, experiences and expectations; develop recommendations that address the issues and challenges that confront consumers and that improve the quality of their experience; and prepare guidelines so that consumers are well informed about cloud products and services. The targets of investigation were individual rather than business consumers. The project has also focused primarily on software, storage, backup and computing personal cloud services, and excluded email, social media, online television and other cloud-based online services.

The objectives of this project were to:

- collect data on consumer contracts, and compare and analyse the terms of services of personal cloud providers to develop guidelines for consumers in relation to choosing a personal cloud provider;
- analyse adopters and non-adopters of personal clouds through a series of focus groups and a national survey of rural communities, IT professionals, non-IT professionals, students and other communities to highlight consumers' awareness, behaviour, experiences and expectations regarding the implications of the personal cloud;
- engage with consumer advocacy groups as well as telecommunications and personal cloud providers to advance their understanding of consumers' emerging needs and issues related to personal clouds, and to support their advocacy and quality (e.g. latency, privacy and security) of services;
- evaluate existing telecommunications consumers' protection and privacy codes in view of the experiences and expectations of consumers; and
- produce policy recommendations and best practice guidelines directed at consumers, consumer advocacy groups, government departments and telecommunications providers.

LITERATURE REVIEW

Diffusion of the Personal Cloud

The diffusion of the personal cloud has been influenced by a number of factors including:

> a burgeoning number of smartphones, personal computers, and other devices, an exploding number of 'easy to use' web services; the growing archive of permanent digital records; the growth in volume and size of digital files; blurring boundaries between work and home and widening variety of digital files and formats. (Gillett et al. 2011: p2)

According to Jun, Lee and Young (2013), 150 million people were using cloud services in 2011 and 375 million in 2012. The number was expected to exceed 625 million in 2013 and more than a billion people by 2016 (Jun et al. 2013). With so many personal cloud products on the market, Pyramid Research estimated that the number of global personal cloud accounts increased 60% over the 2012–2013 period and was expected to grow at a compound annual growth rate of 25% from 2013 to 2018 (Pyramid Research 2014).

Evidence from Australia and the US (ACMA 2014; Gartner 2012) suggests that the majority of consumers use webmail and other software applications. Less frequently used services were storage services, online backup services, computing services and file contact and calendar synchronisation services (ACMA 2014; Gillett et al. 2011). For example, in a survey ACMA conducted in 2013, 88% of the sample used webmail, 40% accessed online software, 36% streamed content, 35% backed up and stored files online and 24% shared files online (ACMA 2014). In another study involving 67 million information workers in America, participants were asked to identify the personal cloud services that they used at work. It was estimated that 41% of the US information workers (around 27 million people) were using one or more personal cloud services, such as office productivity, online storage or file sharing, contact and calendar synchronisation, online backup services and file synchronisation (Gillett et al. 2011).

Benefits of the Personal Cloud

Although the literature reports numerous benefits of cloud computing generally, our review has revealed a lack of focus on the personal cloud and the consumer perspective. For example, numerous articles focus on cloud computing in relation to enterprise customers (Ried, Kisker & Matzke 2010). Indeed, the dominance of the enterprise perspective versus the individual consumer perspective in current cloud computing research was evident in the articles we identified reporting the effect of the personal cloud on enterprises. For example, Ried et al. (2010) predicted that the increasing IT literacy of consumers would result in the integration of private and business lives, which would in turn increase the technology expectations of business users for immediate universal access and unlimited scale. Other articles identified that employees' behaviours in using the personal cloud may put corporations 'at risk' (Ky 2014). Our initial review of the literature identified only a few articles that focus more specifically on the benefits of the personal cloud for consumers (see Table 1).

Although some of the benefits of cloud computing may transcend both business and personal contexts, understanding the 'usage domain' is an important element in understanding personal cloud benefits (Hobfeld et al. 2012). Importantly, there may be benefits of cloud computing that are unique in the personal cloud usage domain. For example, Gnesi et al. (2014) described the concept of a user-centric (v. organisation-centric) data ecosystem to enable individuals to manage the data that are gathered, used and shared about them. Individuals can disclose their address to organisations via their personal cloud and, upon moving house, only need to update the address once to inform all organisations (Hon, Millard & Walden 2012).

Table 1 Summary of literature on the benefits of personal cloud

Benefits	Description	Theoretical Study	Empirical Study
Availability/ mobility	Data redundancy at multiple geographical locations and available through various mobile devices	(Bhattacharyya, Sen & Agarwal 2012; Na, Park & Huh 2010)	
Simplicity	Frees the consumers from detailed capacity planning and eliminates the need to over provision for storage that may be needed; users only need to have internet to benefit from a variety of services	(Bhattacharyya, Sen & Agarwal 2012; Gillett et al. 2011)	(Marshall & Tang 2012)
Cost efficiency	Avoidance of capital expenditure on hardware, software, personnel maintenance; integrated with existing infrastructure	(Rivera 2010)	
Accessibility	Universal and synchronised data access from independent geographical locations	(Bhattacharyya, Sen & Agarwal 2012; Na, Park & Huh 2010)	(Marshall & Tang 2012)
Platform independence	Data access regardless of platform used, such as iOS, Android and Windows	(Na, Park & Huh 2010)	
Self-service infrastructure ease of use	At the customer end, all that is needed to manage storage implementation is a simple web browser, leaving the headaches to the service providers	(Na, Park & Huh 2010)	
Automation	Upgrades, backups		(Drago et al. 2012)
Reliability, security and privacy	Increased security, access to the latest upgrades, integrated management and backup	(Gewirtz 2013; Kuyoro, Ibikunle & Awodele 2011)	
File sharing and collaboration	Empowers users and enables new mobile collaborations	(Gartner, 2012; Li et al. 2010)	(Marshall & Tang 2012)

Factors that Influence Personal Cloud Adoption

The factors that either facilitate or inhibit the adoption of the personal cloud can be grouped into individual, vendor, regulatory and cross-cutting issues.

Individual factors

Moqbel, Bartelt and Al-Suqri (2014) conducted a survey of 265 students and identified that compatibility, social influence and perceived familiarity affected the students' intentions to adopt the personal cloud. Jun, Lee and Young (2013) reported that consumers' self-efficacy, that is, their confidence in, and judgement of, their ability to choose and use a personal cloud effectively influence their intention to use a personal cloud . Vandenbroucke, De Moor and De Marez (2013) undertook an online survey that returned 349 responses. The study revealed that availability, accessibility, privacy and security, cost efficiency (typically 'free' services), sharing data and backup are important features. Some users are unaware of audit rights on their own data or on the personal cloud service provider, and this must be understood before agreeing to the contract; however, a personal cloud service provider may refuse to agree to consumers' terms (Hon, Millard & Walden 2012).

Mohammed (2011) argued that, for many consumers, ease of implementation and use is more compelling than cost factors in adopting the personal cloud. As stated by Wattal, Racherla and Mandviwalla (2010), network externality is another driver that influences consumers to adopt new technology. Thus, for example, individuals might choose to use Dropbox because their network, group or peers are using it too.

Vendor-related factors

Cloud bundling, which means having the services readily embedded within consumer devices, is a popular trend that was identified as another key driver for the increase in adoption of personal cloud services (Ky 2014). Such a cloud bundled service model was adopted by consumer-device vendors, such as Apple with iCloud and Samsung with Dropbox, now followed by other vendors, such as Motorola with Google and Nokia with Microsoft (Steger & Funambol 2012). The interoperability of vendor services and the ownership of space inside the cloud, which is still an unresolved issue, have the potential to derail mass adoption of cloud computing (Mohammed 2011).

According to Hobfeld et al. (2012), vendors' quality of service as experienced by consumers has the potential to become the guiding paradigm for managing quality in the cloud. The reliability and performance of services are susceptible to unpredictable changes in the quality of service depending on the geographic location, type of traffic, file size and hour of the day (Gracia-Tinedo et al 2013). If performance levels do not match consumer expectations because quality is compromised too much, customers will reject the service or refuse adoption. Conversely, meeting or exceeding expectations enhances a cloud provider's reputation and increases levels of utilisation and adoption (Hobfeld et al. 2012).

Interoperability and standardisation of services affect consumers' ability to extract their data and programs and move to another provider easily (ATSE 2010). Consumers who keep large amounts of data would find it either impossible or unattractive to switch from one type of service to another or

from one vendor to another (Jun, Lee & Young 2013). Further, contract lock-ins, exit conditions and termination rights are additional challenges for consumers when they intend to discontinue using a service (Lewallen 2013).

Institutional factors

Different governments and consumer protection agencies or groups around the world can play important roles in regulating or influencing the adoption and use of cloud computing in general and personal cloud services in particular (ATSE 2010). At the international level, there have been initiatives to develop international frameworks and the explicit requisition of international standardisation (Marnau et al. 2012).

In the US, the Consumer Federation of America (CFA) released a list of best practices for consumer protection in cloud computing services (CFA 2010):

- 'Free' services should have the same consumer protection standards as paid services.
- Consumers should be able to delete information they upload to the cloud.
- Personal cloud service providers must demonstrate operational safeguards and data security mechanisms through expert audit and certification.
- Service providers must clearly disclose the secondary usage of consumers' personal data with 'technical justifications' or 'business justifications'.
- Portability is a key for competition in cloud services; personal cloud service providers should not interfere with interoperability.
- Personal cloud service providers should be transparent about basic information such as the level of service provided, the business model of the personal cloud service provider, the legal protections that apply to data and who to contact if questions arise.
- For law enforcement, users should receive notice of criminal and civil requests for information and access to their data.

In Europe, the European Consumer Organisation has highlighted three key aspects in relation to consumer data protection legislation to raise their trust on cloud services: (1) transparency: consumers need to know what will happen to their personal data in the cloud; (2) applicable law: consumers need to be confident that their rights will be protected by European law, not by offshore jurisdiction; and (3) law enforcement: consumers need to be confident that their personal data in the cloud will not be given to third-country administrations (BEUC 2013). European data protection law requires data controllers (organisations with the responsibility for deciding what happens with personal data) to implement appropriate technical and organisational measures to protect personal data from security breaches and breaches of confidentiality (BEUC, 2013).

In Australia, existing warranties in the ACL against services that are not fit for purpose, and against false or misleading representations of products or services, are actionable under the ACL, as well as contract law. The *Australian Privacy Act*, which came into force on 12 March 2014, imposes new obligations on companies that collect and process personal information, including those that operate cloud services. Indeed, the government is closely monitoring the cloud services market to ensure that consumers take full advantage of cloud services (DBCDE 2013).

Cross-cutting issues

Studies have also explored the security, privacy and trust concerns of personal cloud users (Na, Park & Huh 2010). The cloud environment is exposed to a number of direct security threats, such as the abuse and nefarious use of cloud computing, insecure interfaces and application programming interfaces (APIs), malicious insiders, data loss or leakage, and account or service hijacking (Na, Park & Huh 2010). Research has shown that it is easy for consumers to abuse a cloud service by aggregating free accounts from one or several providers to obtain a high-quality storage service and better transfer performance for malicious use (Gracia-Tinedo et al. 2013a). To prevent such security risks, cloud providers should seriously consider the implicit risks of their free services and open APIs (Gracia-Tinedo et al 2013a). However, there are fears that cloud service providers might not provide as many security features to individual consumers as they would to enterprise cloud users (Bhattacharyya, Sen & Agarwal 2012).

Commonly, consumers fail to take into account possible privacy consequences in choosing and using the personal cloud (Fahl et al. 2012). Data may be stored at multiple locations across several jurisdictions with differing privacy and data protection legislation. Personal cloud service providers often prefer to locate their data centres in jurisdictions with minimal legal requirements (ATSE 2010). From the consumers' perspective, there are protocols that force personal cloud service providers to disclose the locations of their data centres, but consumers do not usually take this into consideration when placing their private information into personal cloud services (ACS 2013b). The laws and recommendations that provide guidelines under an organisation-centric model on how organisations can collect and process data related to their customers or users are not clear for user-centric models, and regulations of personal data in the context of personal cloud services are yet to mature (Gnesi et al. 2014).

Trust is both a major driver and a constraint for secure cloud computing (Mohammed 2011). At present, consumers' trust is an issue, with its basis in legal uncertainty of applicable laws on cloud issues, possible enforcement and the lack of appropriate redress in case of disputes (Hustinx 2012; Martic 2013). Trust behaviour must have a legal enforcement or standards basis that includes security and privacy measures (ATSE 2010). Service level agreements (SLAs) can provide an integrated approach that can be used to build trust between personal cloud service providers and consumers (ATSE 2010).

METHODOLOGY

This project was conducted using a mixed method strategy of interviews, focus group discussions, Q-method interviews, a survey and desk research.

Interviews

To obtain providers' and advocacy groups' perspectives, nine interviews were conducted during October–November 2014 with industry, government and consumer representatives. Three of these interviews were informal; participants agreed to discuss the interview questions but did not wish to be identified or quoted in the formal reporting of the study. The interviews explored the organisations' interest in the personal cloud, how personal cloud products are packaged and priced, the most important issues that consumers need to be aware of in choosing and using the personal cloud, potential competition issues in cloud computing, and the key role of government and wider consumer organisations.

Out of the nine interviews, four (three formal and one informal) were with owners and managing directors of personal cloud providers, two interviews were with managers working in two consumer group organisations and three interviews (two informal) were conducted with managers from two regulatory agencies. Appendix A provides further profiles of the participants of the formal interviews. All formal interviews were audio recorded and then transcribed by a professional transcription service. The transcripts were then analysed using qualitative content analysis to identify key themes.

Focus Group Discussions

To identify early adopter consumers' experiences, six focus group discussions, each lasting 75–90 minutes, were held with 29 participants (13 female) from different consumer categories in October–November 2014. The discussions were aimed at discovering consumers' understanding of the personal cloud, the personal cloud services that they used and on what basis they made this choice, how much they spend on the personal cloud, what key things they consider in personal cloud contracts, negative experiences and positive benefits associated with personal cloud use, and what they would like to see in the personal cloud market.

Ten of the participants in two focus groups were non-IT professionals from a variety of professions, including a librarian, hairdresser, musician, administrator and finance worker. Another 10 participants in two groups were IT professionals working as a business analyst, digital marketer, enterprise architect, solution consultant, data analyst and academic. The remaining participants were university students undertaking undergraduate- or postgraduate-level studies. The profile of the focus group participants is in Appendix A.

Q-Method Interview

To identify the most and least important personal cloud issues, a Q-method interview was applied. A Q-method interview is a structured interview technique to segment participants into distinct groups

using their responses to a card-sorting activity (Thomas & Watson 2002). Based on the literature review and exploratory interviews, 63 personal cloud–related issues were identified. Twenty-six new participants (20 males and six females with the age range of 24–69 years) that were not part of the focus group interviews completed the Q-interview sessions during January 2015 (Appendix B). All participants were asked to (a) provide background information about themselves and their personal cloud use, (b) sort the importance of the 63 statements using a 15-point 'Q-scale' that ranged from –7 (most unimportant) through zero to +7 (most important) (see Appendix C), and (c) give reasons and justifications for ranking and sorting the statements. To improve the credibility of the results, participants were given a chance to change and confirm their sorting if there was any discrepancy between the ranks of the sorted cards and their explanation. Each interview lasted an hour. The output of each Q-interview session produced a score sheet (see Appendix D) that sorted and ordered the importance of the 63 items. The data were analysed using the statistical tool 'R with Q-method' package.

Survey

Data were also collected from a survey of Australian consumers in March 2015. The survey had two sets of questionnaires for personal cloud user and non-user consumer groups. The questionnaire was developed based on the findings of the review of the literature, exploratory interviews and Q-interviews. The users' survey had 95 questions and the non-users' survey had 57 questions. In both surveys, seven questions were used to capture the demographic details of the participants in terms of gender, age, income, education and residence.

The sample was selected from the Research Now (an international panel company with an office in Australia) panel of 'everyday consumers'. We chose Research Now as it provides 'the largest, highest-quality survey sources available to researchers'. The sampling criteria were Australians above 18 years old with a national representation of gender and location equally divided between users and non-users of the personal cloud. To identify the users of the personal cloud from non-users, we provided a definition and description of the personal cloud in the questionnaire and asked consumers to self-nominate if they had ever used any one of (a) backup as a service, (b) storage as a service, (c) software as a service or (d) computing as a service personal cloud services. Based on their responses, they were directed to complete either the user or the non-user survey.

A total of 8,700 consumers were invited to participate in the survey and 1,237 attempted it; 284 responses were incomplete and excluded from the analysis. IP addresses and latitude and longitude identifiers were used to prevent multiple responses from a single respondent. Of the 953 consumers that completed the survey, 479 were current users and 474 non-users, 58% were females, 54% were in the 18–35 age group, 43% earned less than $37,000 annually and 52% had a high school or technical and further education (TAFE) qualification. The majority (60%) were from New South Wales and Victoria, 58% lived in urban areas, 28% in regional areas and the remaining in rural and remote locations. A further demographic breakdown of the survey respondents is shown in Table 2.

Table 2 Demographic profile of survey participants

Category	Description	Count	Percentage
Personal cloud status	User	479	50.3%
	Non-user	474	49.7%
Gender	Male	402	42.2%
	Female	550	57.7%
	Other	1	0.1%
Age	18–25	203	21.3%
	26–35	315	33.1%
	36–45	157	16.5%
	46–55	92	9.7%
	56–64	84	8.8%
	>65	102	10.7%
Education	Primary	8	0.8%
	High school	249	26.1%
	TAFE	248	26.0%
	First degree	329	34.5%
	Masters	110	11.5%
	PhD	9	0.9%
Income	0–$18,200	222	23.3%
	$18,202–$37,000	192	20.1%
	$37,001–$80,000	372	39.0%
	$80,001–180,000	151	15.8%
	$180,001 and over	16	1.7%
Residence	Urban	555	58.2%
	Regional	270	28.3%
	Rural	123	12.9%
	Remote	5	0.5%
State	New South Wales	294	30.8%
	Victoria	277	29.1%
	Queensland	186	19.5%
	South Australia	77	8.1%
	Western Australia a	65	6.8%
	Australian Capital Territory	28	2.9%
	Tasmania	22	2.3%
	Northern Territory	4	0.4%

The majority of the respondents (59%) were between 26 and 55 years. This is slightly higher than the national age structure of 42% for the 25–54% age group. Nine per cent and 11% of the responses were from the 56–64 and 65 years and over age groups respectively, mirroring the national distribution of 11.8% and 14.4% respectively. Based on the Australian and New Zealand Standard Classification of Occupations (ANZCSO), 24% of the participants were professionals/technicians, 22% worked in administration, sales and communality services, 10% were managers and 3% were labourers or machine workers. The remaining were house makers or retired (17%), students (10%) and not specified (14%).

Desk Research

To evaluate existing consumer protection and privacy codes in view of the experience and expectations of consumers of the personal cloud, a number of documents were reviewed. These include the *Australian Competition and Consumer Act 2010,* the *Australian Consumer Law 2011*, the *Telecommunications Act 1997,* the TCP Code 2012 and the *Australian Privacy Act 1998.* We also considered the Meta Data Retention and Use Bill 2015, the *National Cloud Computing Strategy* (DBCDE 2013), the ACS's national cloud computing protocol (NCCP) report (ACS 2013a, 2013b), the Department of Communication's regulatory stocktake report (DOC 2014) and information available from the websites of the Australian Communication Media Authority and Australian Competition and Consumer Commission (ACCC). Further, the terms of services and privacy policy statements of 11 cloud providers were reviewed.

FINDINGS AND DISCUSSION

A Taxonomy of Personal Cloud Services

The personal cloud encompasses four different types of experience through which consumers store, synchronise, stream and share content on a contextual basis regardless of device or platform (Gartner 2012). To obtain the four different experiences, consumers can choose from different personal cloud deployment and service models. The deployment models can be categorised into two groups: private personal cloud and public personal cloud.

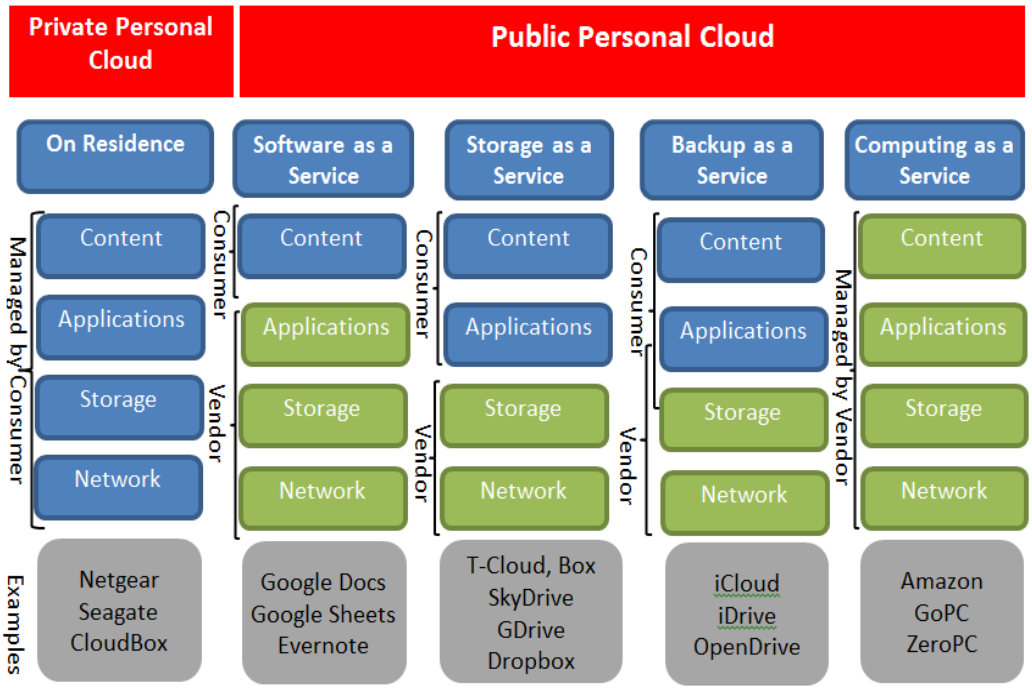
In the private personal cloud environment, consumers install and connect devices to back up multiple computers; keep digital content; wirelessly access content at home or on the go and stream it to other home devices, such as gaming consoles, media players and smart televisions; and share content with friends and family. In contrast, public personal clouds refer to four main types of vendor-provided service models: software as a service, storage as a service, backup as a service and computing as a service.

- Software as a service: vendor software programs deployed in a public cloud, which consumers use based on subscription, without the need to download or install them on their computers. The subscription fee also covers assistance from the service provider. Examples include Google Docs, Google Sheets and Evernote.
- Storage as a service**:** an online space provided to the public, usually through a premium pricing model, to store, back up and share digital content**.** Although some of the software as a service models incorporate storage as a service, not all storage as a service models offer software. Examples include T-Cloud, Google Drive, Dropbox, SkyDrive, OneDrive, Amazon Cloud Drive, Box and JustCloud.
- Backup as a service: a service to back up digital content and devices. Examples include iCloud, iDrive and OpenDrive.
- Computing as a service: computing services that recreate a personalised setting of a consumer's desktop with an online version accessible from anywhere through the internet. Many computing as a service models provide the capability to synchronise regular desktop and webtop versions. Examples are Amazon and GoPC.

Consumers have more control with private clouds than they do with public clouds but lack offsite backup. In a private cloud, consumers can customise security systems and applications and have greater control (Hon, Millard & Walden 2012). With standardised applications, the public environment offers consumers little control, and they have to rely on vendors to secure applications, as well as the environment (Hon, Millard & Walden 2012). Figure 1 shows a diagrammatic representation of the different personal cloud deployment and service models and the extent of consumers' control.

Figure 1

Types of personal cloud services



When presented with the abovementioned types of personal clouds, the interview and IT savvy focus group participants more or less agreed with the public personal cloud typology. However, there was no consensus on whether the concept of private personal cloud makes sense. Some consumers and providers tended to see the private personal cloud as a 'personal network' rather than a personal cloud but others disagreed:

> *'Cloud is more of a large-scale network where multiple users actually have data stored and often times where that data is stored is—even though the boundaries of that cloud is obviously defined it's not clear exactly which server it is at any point in time to the user ... that is what I would define as a cloud; a network of devices and storage units as an external provider rather than a personal network that I own regardless of the fact that I can still access both of them over the internet…. So in your definition, when you split the two, I would call the larger scale one as a cloud and the other one as a personal network.' (Consumer 18)*

> *'Why can't we draw a parallel? If you have private cloud in an enterprise sense where only few enterprises can access it, and when you creating your own cloud and your personal space and allow your social group and a few members of your family to access it over the internet. So why can't we call that a private cloud—a private personal cloud?' (Consumer16)*

In addition to the use case, which is one element that makes a cloud a personal cloud, the freemium pricing model, the level of encryption strength, the complexity of managing accessibility perimeter, the non-negotiability of the terms of service and the configuration of the service in terms of scale, and traceability differentiate personal clouds from enterprise clouds.

Consumers' Awareness of the Personal Cloud

The personal cloud landscape is not simple. There are many options with specific advantages and disadvantages (Drago et al. 2013; Gillett et al. 2011). Consumers' awareness of these options is the foundation to an effective cloud experience. In addition, consumers' level of awareness of data location and retrieval, legal and regulatory issues, and the performance, conformance and reputation of service providers affect cloud adoption (AGIMO 2014). Consumers are reportedly using a range of cloud services without recognising that they are doing so.

> *'One of the things we have found, out of all of this, is that there's actually very wide use of cloud services, but consumers, generally, don't recognise that they are using cloud services. When they are using Gmail for example, that's a cloud service and people wouldn't relate that to a cloud service. I think a lot of what people relate to cloud is often that sense of business data storage, but not understanding the range of services that they may be accessing that are actually housed or stored in the cloud.' (Regulator 1)*

Consumers demonstrate different levels of awareness regarding cloud-related issues. On balance, the average consumer has a limited understanding of how personal clouds work, what they offer, and what they mean for data security and privacy. A female focus group participant shared her confusion as follows:

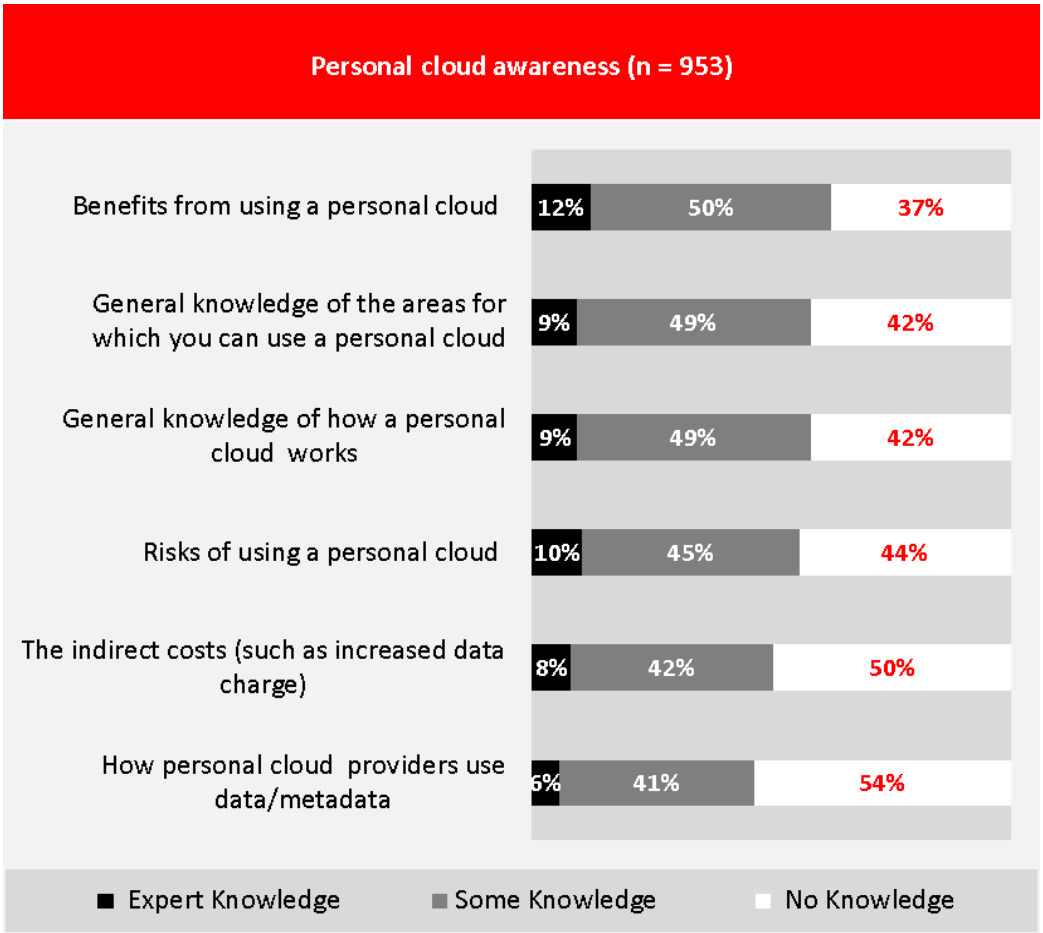
> *'When we talk about the personal cloud, in terms of the way it's being portrayed by the media it often has quite negative connotations. However, in reality, I actually don't quite understand what the personal cloud is because it's not tangible. So for me, visually, I see it as a cloud, in my mind it's a cloud.' (Consumer 1)*

The survey findings (see Figure 2) also reveal that 85% of the surveyed consumers that used the personal cloud did so without, or with very little, understanding of how service providers use their data or metadata, or the risks involved and the precautions to be taken in using a cloud service. Gender, age, education and income had a statistically significant influence on personal cloud awareness. Together, these four factors explain a quarter of the variation in consumers' awareness, with age being the most important of all:

- In general, older people were two times less aware than those in the 26–35 year age group.
- On all six questions, male participants showed relatively higher awareness than female.
- There was a positive association between the level of formal education and the level of personal cloud knowledge. For instance, in terms of general knowledge about when and where to use a personal cloud, respondents with primary and high school education had the lowest level of awareness. The highest level of awareness belonged to the respondents with a master's or above degree. In terms of knowledge on how personal cloud services work as well as the risks, respondents with university education had better knowledge than respondents with a primary or high school education.
- Awareness of the what, why, how and benefits and risks of the personal cloud also increased with income. Of those earning $80,000 and above, 71% were aware of the benefits of the personal cloud compared with only 54% of those earning less than $18,500. Only 38% of consumers with income less than $18,500 understood how their data are used compared with 66% earning above $80,000.

- Although urban dwellers showed a slightly better understanding of personal cloud than non-urban dwellers (for example, although 60% and 66% of urban dweller respondents were aware of the risks and benefits of personal cloud respectively, only 50% and 57% of non-urban dwellers did so), the difference was not statistically significant.
- Non-users demonstrated a markedly lower level of personal cloud awareness. For example, when asked about their general knowledge of the areas for which they can use personal cloud services, 67% perceived they had no knowledge. Only 2% of the non-users perceived that they had expert knowledge of how personal clouds work. Ninety-eight per cent of non-users did not understand or had a very shallow understanding of how cloud providers use data and metadata. Two out of three non-users identified that they did not understand the indirect costs, risks or benefits of personal clouds. These suggest that lack of awareness may affect the non-adoption of personal cloud services.

Figure 2 Personal cloud awareness



A few consumers understood that providers offered 'free' services to them because providers often earn revenue from advertising to them. They also had some insight around how providers share their data to other organisations; however, they did not necessarily understand how those shared data were ultimately used. A provider offered the following observation:

> *'People—the average Australian doesn't understand how valuable their data is or what it's used to increase things like their insurance costs.... For generations of children that are being*

born now it may be used to either allow them to have a university education or disallow that; for them to get medical treatment or not.' (Provider 2)

Personal Cloud Use

Consumers can use the personal cloud in four major areas: (1) to create and access content anywhere on multiple devices, which makes cross-functional collaboration in document creation and formatting or editing much easier; (2) for storage or backup of content such as documents, pictures, movies, video or audio; (3) to share digital content with others without the need to keep multiple copies; (3) to synchronise content and applications across devices and applications; and (4) to stream pictures, news, audio and video files (Ardissono et al. 2009; Gartner 2012).

As shown in Figure 3, out of the 479 personal cloud users, more than 80% used cloud storage and backup services and two-thirds used cloud software to create and manage digital content. Nearly one in two consumers used a do-it-yourself private personal cloud, either on its own or in addition to a public personal cloud. Whereas less than 12% of over 55s had adopted this model, 50% of 18–35 year olds were using it. Interestingly, 80% of consumers with PhD degrees did not use a private personal cloud, whereas 75% of those with primary education and 47% of urban and non-urban (regional, rural, remote) dwellers did.

Computing as a service models were used by less than half of the 479 survey participants. This model was chosen by 56% of males, 36% of females; 47% of non-urban and 43% of urban dwellers. In addition, such models were used more by consumers earning above $80,000 (57%) than those earning less than $37,000 (30%). Among the urban dwellers, the two most frequently (80% and above) used services were storage (86%) and backup (81%) services. Among the non-urban (regional, rural and remote) dwellers, the order changed to backup (85%) and storage (81%). However, these percentage differences between urban and non-urban dwellers were not statistically significant.

Figure 3

Frequently used personal cloud models

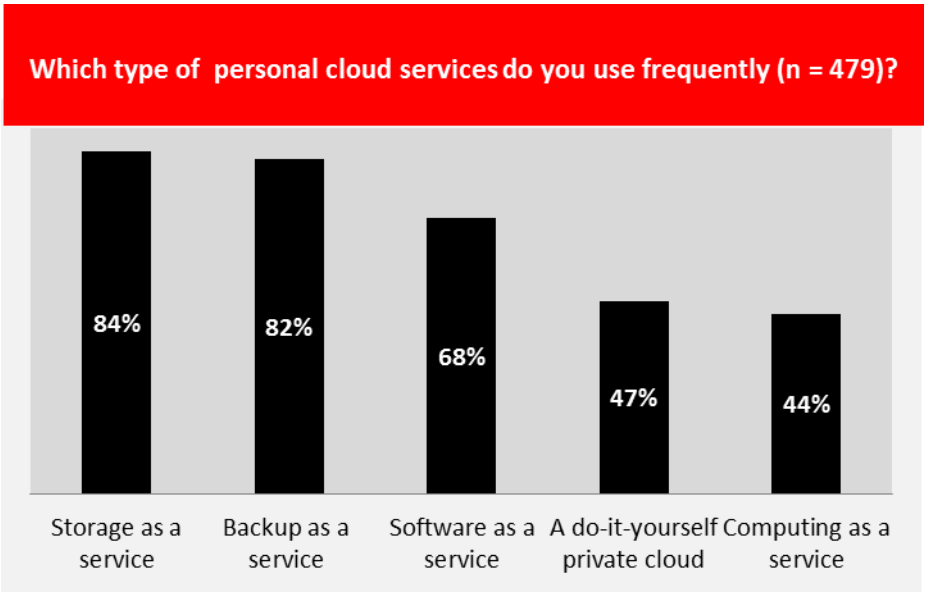


Table 3 documents a further breakdown of the specific cloud services the 479 survey respondents were using (note that in the table, the total is greater than 480 as consumers were asked to list the three most frequently used services).

Table 3 Personal cloud services used by consumers

Cloud Type	Number of Responses	Percentage (n = 479)	Cloud Type	Number of Responses	Percentage (n = 480)
iCloud	214	44.6%	Adobe Creative Cloud	3	0.6%
Dropbox	189	39.4%	Hotmail	3	0.6%
Google Drive	131	27.3%	Samsung backup	2	0.4%
OneDrive	45	9.4%	Photobucket	2	0.4%
Google Doc	41	8.5%	OpenDrive	2	0.4%
SkyDrive	24	5.0%	Office 365	2	0.4%
Google Sheets	17	3.5%	SafeSync	2	0.4%
Evernote	14	2.9%	Seagate	2	0.4%
Amazon	14	2.9%	4shared	2	0.4%
iTunes	12	2.5%	UCloud	1	0.2%
Private cloud	10	2.1%	Moodle	1	0.2%
Telstra(T-Cloud)	7	1.5%	GoPC	1	0.2%
WD My Cloud	6	1.3%	Flicker	1	0.2%
OpenDrive	5	1.0%	Creative Cloud	1	0.2%
MediaFire	5	1.0%	ZipCloud	1	0.2%
Yahoo	5	1.0%	Synology NAS	1	0.2%
iDrive	4	0.8%	TeamViewer	1	0.2%
IBM	4	0.8%	SoundCloud	1	0.2%
Box	4	0.8%			

The results indicated that the most common choices were iCloud, Dropbox and Google Drive. This means the consumers tended to choose global personal cloud providers that offer a range of bundled services and rich experience over Australian providers that offer niche services, even if Australian providers' servers are located in Australia and governed by Australian consumer and data protection regimes. A male focus group participant explained the rationale for using Google personal cloud services:

> *'Google has become an ecosystem. So if you had a Gmail account you could use Google Drive, for example. That storage is shared and it makes it very easy. You can even save your attachments that come through to your Gmail into your Google Drive. Then you can share them with other Google users. That allows you—the same login allows you to have an Android phone, which you can hook up. So it's become, like, an ecosystem of services as well as other software. So there's—one account provides you access to many things.' (Consumer 19)*

The difficulties Australian start-up personal cloud providers face in offering an integrated service that competes with global providers was indicated by one provider:

> *'Most people want to run Microsoft Office, and it's like well this is identical. Yeah but I want Microsoft Office, well in that case we have to spin up a machine with Microsoft, we have to*

pay the Microsoft tax. Oh that's expensive, yes it is. So what we need to do is basically we need to make our messaging on the website clearer still, and refine the sales funnel, so that we're screening people earlier.' (Provider 1)

The personal cloud services that consumers use differ in terms of free storage size, the maximum file size and data centre location. Table 4 shows a comparison of a sample of public personal cloud services from each service model category.

Some consumers also use personal clouds without necessarily knowing that they are using them. In particular, cloud services that are bundled with device purchases, such as iCloud from Apple, OneDrive from Microsoft, Google Drive for Android, fall into this category. A female focus group participant shared how she believed her iCloud works:

'But you know, some of it happens automatically, I don't do it consciously and it's because I don't have enough knowledge or experience to know how to go about physically saving it myself. I know it happens but my knowledge is very little for me to know when it happens, when it doesn't happen. I don't actively go out searching to save things on the iCloud.' (Consumer 5)

This trend could be common among many consumers as the non-user survey results showed that the majority (66% of 474) did not necessarily recognise when they were using a personal cloud service and only 14% reported knowing when they were using a cloud; the rest were unsure about whether they knew or did not.

Table 4 Comparison of a sample of personal cloud services (as of June 2015)

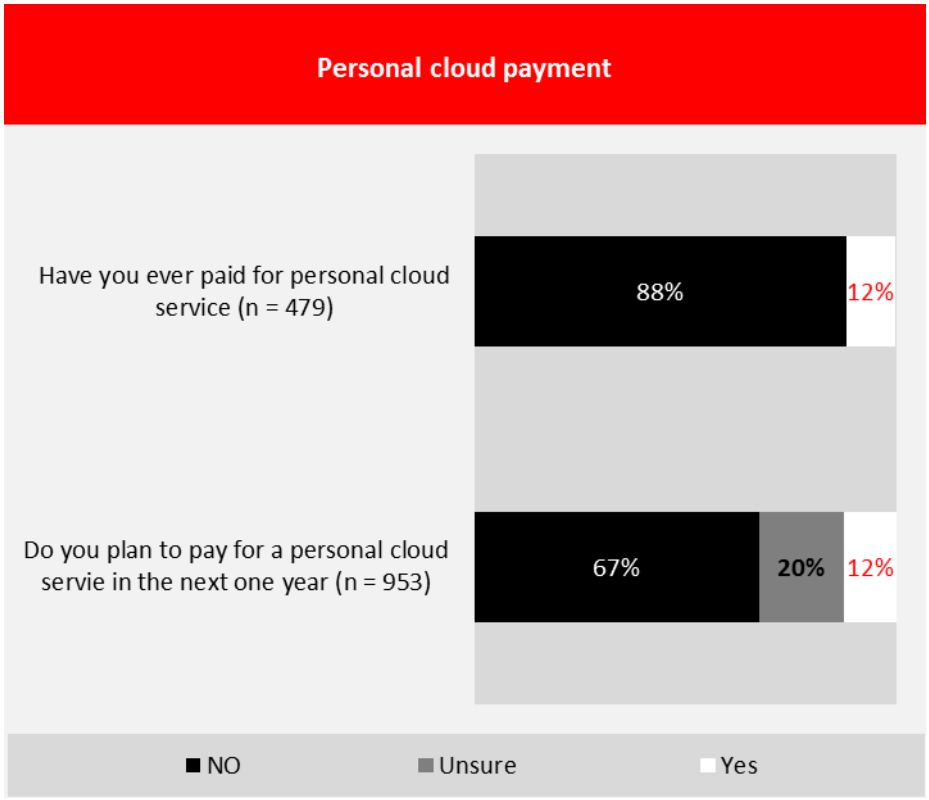
Criteria	Evernote	Dropbox	Google Drive	iCloud	GoPC	Onexus	Meeco	Cloud Drive	OneDrive	Box	T-Cloud
Free storage	60 MB/month	2 GB	15 GB	5 GB	None	None	None	None	15 GB	10 GB	None
Monthly subscription fee	US$2.5 = 1 GB US$5 = unlimited	AU$12.99 = 1 TB	US$1.99 = 100 GB US$9.99 = 1 TB US$99.99 = 10 TB US$199.99 = 20 TB US$299.99 = 30 TB	US$1.29 = 20 GB US$4.99 = 200 GB US$12.99 = 500 GB US$24.99 = 1 TB	AU$20/user = 20 GB AU$35/user = 50 GB	US$30 one-off fee	N/A	US$19.99 = 5 GB + unlimited photos US$59.99 = unlimited	AU$2 = 100 GB AU$4 = 200 GB AU$9 = 1 TB	US$10 = 100GB	AU$5 = 30GB AU$10 = 70GB AU$30 = 300GB
Maximum file size	Not disclosed	10 GB	No limit	No limit	Not disclosed	Not disclosed	N/A	2 GB	10 GB	250 MB	No limit
Where files stored	USA	USA and Ireland	USA, Asia and Europe	USA, Ireland, Denmark	Not disclosed	USA and others	Australia	Not disclosed	USA and others	USA	Australia
Synchronisation	Auto sync on all devices	Auto sync on all devices	Auto sync on all devices	Auto sync on all devices	Auto sync on all devices	Not stated	N/A	N/A	Auto sync on all devices	Auto sync on all devices	Auto sync on all devices
Accidental data deletion recovery	Evernote Trash	Dropbox bin	Google Drive bin	Not stated	Every 24 hours Backup	Not stated	Not stated	Deleted folder	Recycle bin	Trash folder	Not stated
Controlling upload/ download speed	Unknown	Available through setting	Available through setting	Available through setting	Unknown	Unknown	N/A	Unknown	Unknown	Unknown	Unknown
Operating system compatibility	Windows, Mac OS, iOS, Android	Windows, iOS, Android	Windows, iOS, Android	Windows, iOS, Android	Windows, iOS, Android	iOS	iOS	Windows, Mac OS, iOS, Android	Windows, Mac OS, iOS, Android, Xbox	Not stated	Windows, Mac OS, iOS, Android
Interoperability with other cloud services	Not supported	Not supported	Not supported	Not supported	Compatible with Dropbox	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated
Help desk location and availability	Chat, email	Forum	Forum	Phone	Phone	Online form	Email	Not stated	Mail	Phone	Phone, CrowdSupport

Premium v. 'Freemium' Cloud Consumers

The majority (88%) of the 479 who completed the users' survey did not pay for cloud services and seemed to be content to stay within the free limits of the providers (see Figure 4). Those that were paying spent on the average $222 per year. A male focus group participant explained why he paid for backup personal cloud services:

> *'I pay heaps for my additional space. I pay about $50 a month on iCloud, so 25 gig, because well it's pointless giving me five gig when I've got a 32 gig iPad and iPhone, you know what I mean. So it's backing up everything that's on there, I can't just—I suppose I can pick and choose but then how do you pick and choose from what … and all that sort of stuff, so it just gets a bit too messy. So when I back up I back the whole thing up.' (Consumer 29)*

Figure 4 **Personal cloud payment**



In addition, only 12% of all the 953 surveyed consumers intended to pay for a personal cloud service within one year after the survey. There were statistically significant differences in consumers' intentions to pay for cloud service due to age, gender, residence and education differences. Of those in the 18–35 age bracket, 18% planned to pay for a cloud service compared with less than 3% of those above 56 years old. Males (16%) and urban dwellers (15%) were more likely to pay than females (10%) and regional, rural and remote dwellers (9%) respectively. Those that had a PhD qualification were two times less likely to pay for a cloud service compared with consumers with primary education. Another male focus group participant shared how he planned to avoid paying for a personal cloud by creating multiple accounts.

'I am not willing to pay for this cloud service, I would rather have three or four Gmail accounts, run three or four different Google Drives, because maybe my plan is different, I just want to store in a different place.' (Consumer 25)

However, consumers' unwillingness to pay for cloud services and the availability of free cloud services are challenging the sustainability of small Australian cloud service businesses, as explained by the manager of one of the cloud services providers:

'We were going with a freemium model, so originally we were a free model, and the thought was to encourage them to come back and actually buy something that high value. Of the 16,000 users, no one really came back.' (Provider 1)

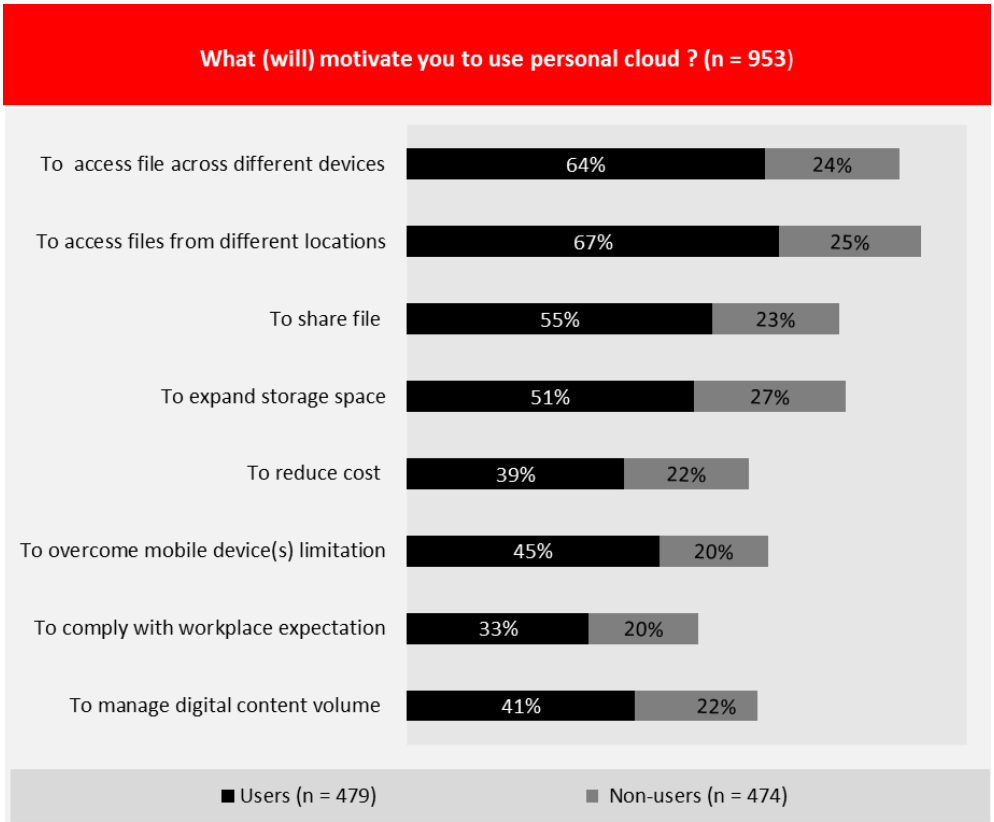
Motivation for Using a Personal Cloud

Users and non-users of personal clouds significantly differed in terms of what motivated them to use a personal cloud (see Figure 5). For users, mobility to access and share their digital content easily from anywhere, anytime and any device were what motivated them primarily to use a cloud, followed by overcoming storage and mobile device limitations. In contrast, 65% of non-users either did not have a need or were uncertain whether they needed a personal cloud. Further, the majority of the non-users were unconvinced, unsure or had yet to encounter the need for mobility across devices and locations. They neither experienced limitation of mobile devices nor believed that a personal cloud is a way to overcome that limitation. Further analysis of the data showed that:

- One in three consumers faced workplace expectation to use a personal cloud. However, only one in five non-users would use a cloud if it became a workplace requirement.
- There were no statistical variations in the motivation due to gender differences but there were some statistical variations due to age. Generally, as age increased, the motivation for a personal cloud decreased. Forty-six per cent of 18–35 year olds were relying on a personal cloud to overcome the limitations of tablets and mobile phones. Forty-four per cent of above 65 year olds used a personal cloud to share files.
- Thirty per cent of consumers earning less than $37,000 were using a personal cloud to reduce the cost of storage and software. Sixty per cent of consumers earning above $180,000 were motivated to manage the volume of their digital content.
- Two-thirds of regional and rural communities and half of remote communities were motivated to use a personal cloud to access files across different devices, whereas two-thirds of urban dwellers were motivated to access files from different locations.

Figure 5

Motivation for the personal cloud



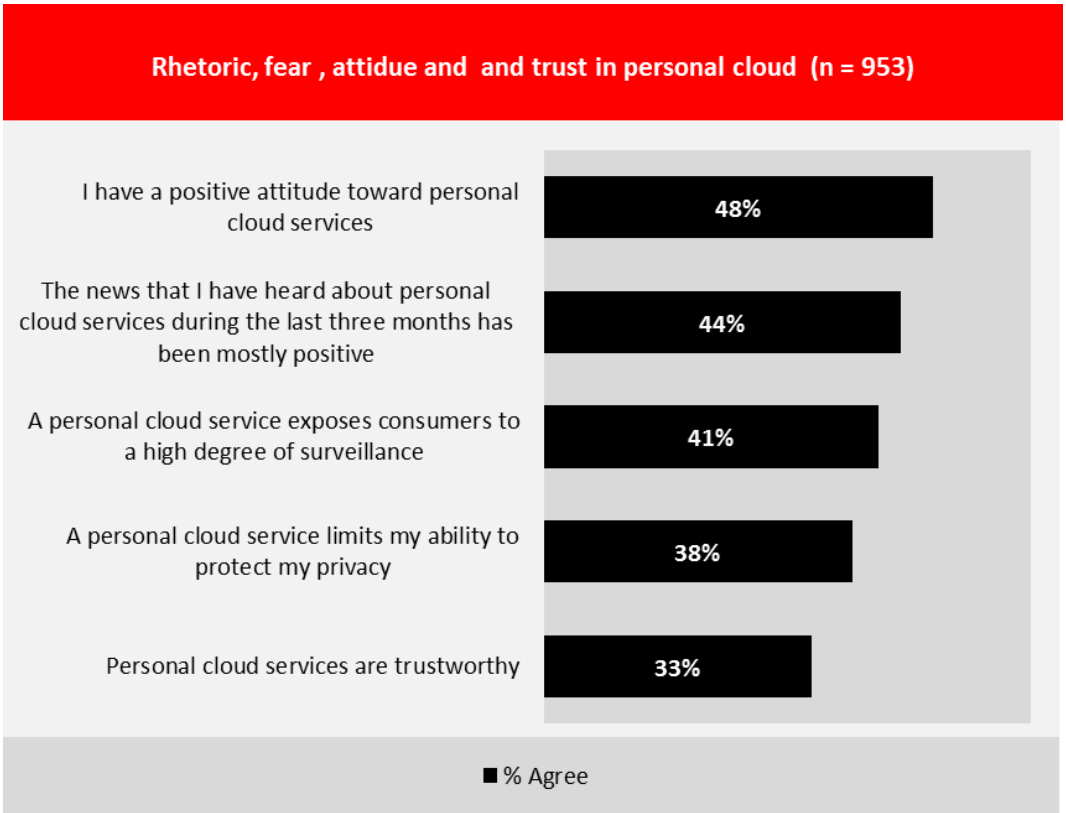
Consumers' Fears and Doubts

The current rhetoric about personal clouds is hardly positive (see Figure 6). In the three months prior to the survey, less than 45% of the consumers had heard positive, good or favourable news about personal clouds. Further, there was a fear (41%) that use of a personal cloud makes the level of surveillance that would have been illegal in the physical world possible in the electronic world. As one interviewee puts it, '*in fact we've provided a low cost service for intelligence agencies all over the world*' (ITSFG2M5). The managing director of a niche Australian personal cloud provider shared these consumers' concerns:

> *'But I think one of the things in any study of personal clouds right now has to come back to sort of the jurisdictional and democratic and judicial roots of a geolocation, and in this case Australia and Australian personal cloud.... Because at the moment we have protection in the physical world ... but what we find is that those democratic rights right now are about to be completely broken in the way that we translate to the digital world; to the things that I can't do to you physically I can do if they are digital. So I can follow you, I can surveillance you, I can monitor you, I can go through your information, your physical whereabouts. I can infer behaviour and I can treat you as if you are 24/7 a suspect of the state even if you are a 17 year old university student doing no more than, you know, contributing to a study or writing a paper'. (Provider 3)*

Figure 6

Personal cloud rhetorical experience, fear, attitude and trust



Consumers were equally divided among those that believed that personal clouds limit their ability to protect their privacy (38%), those that were unsure (30%) and those that disagreed (30%). Despite these differences in opinion, 48% of consumers had a positive attitude towards personal cloud services. Nevertheless, only 33% of consumers considered personal cloud services trustworthy.

There was a statistically significant relationship between awareness and fear of surveillance and attitude but not trust. This indicates that as consumers' awareness increased, their fear reduced and they developed positive attitudes towards the cloud. Nevertheless, more awareness does not necessarily translate to better trust of cloud services. The relationship between attitude towards the cloud and trust was positive and statistically significant, but the contribution of attitude to cloud service trust was small, implying that although having a favourable attitude is important, trusting personal clouds can take much more than awareness and favourable attitude, as explained by a female participant:

> *'I think my view would be that I don't really look at what's safe or not safe because I don't trust anything. I think my view would be that if I'm putting something up I don't care if people see it. That's my view. It's obviously so general that it's not going to be dangerous to me if it's out there. So that's for personal cloud use.' (Consumer 7)*

Consumers' rhetorical experience, that is, the nature of the news that they hear about personal clouds, was another factor that was contributing to their fear of personal cloud–related surveillance. There was a statistically significant and negative relationship between age and attitude towards the personal cloud, indicating that as age increased, the attitude towards the personal cloud tended to

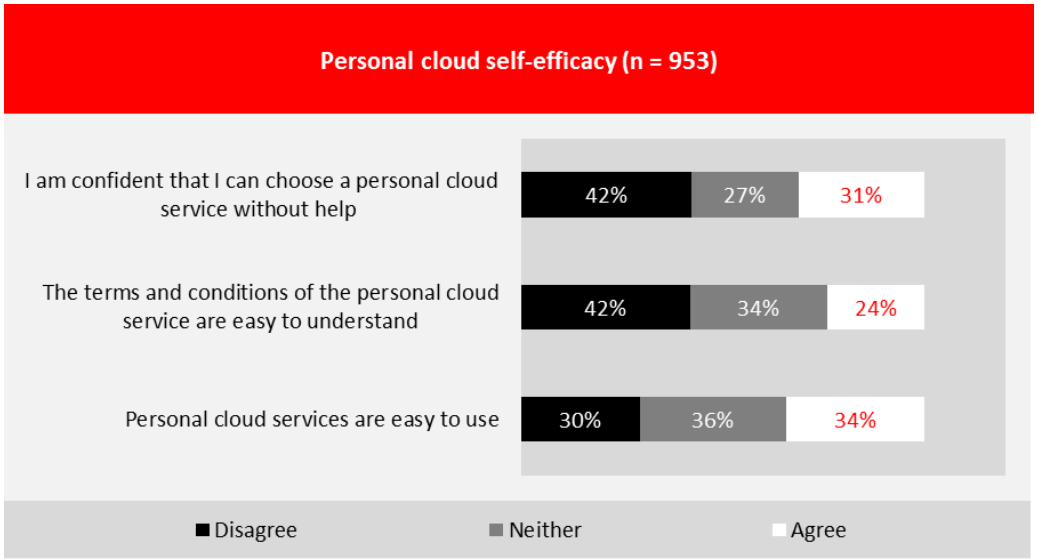
change from favourable to negative. While consumers' education level was positively related to favourable attitude, it was negatively related to fear of surveillance and trust.

Personal Cloud Self-Efficacy

Consumers' self-efficacy, that is, their confidence in, and judgement of, their ability to choose and use a personal cloud effectively is another important factor that influences cloud use (Jun 2013). The survey results indicate (see Figure 7) that only 31% of consumers were confident about choosing a personal cloud without help and one in four consumers found the terms of conditions easy to understand. In addition, 34% of consumers agreed that personal cloud services are easy to use and half of the users doubted their ability to manage their account and set an appropriate level of access to their data.

Figure 7

Personal cloud self-efficacy



Personal clouds are provided under standard form of contracts. These contracts allow service providers to change the performance of their cloud services, such as in size, speed and file delivery mechanisms, without consumers' consent. Most consumers find it overwhelming to read and understand the terms and services. One interviewee described this as follows:

> *'I think what happens is when you start reading them you become so overwhelmed with the wording of it, it's very vague and it can be misleading. For someone who doesn't have technical knowledge…some of the words I don't even recognise, it is jargon. So you just skip, accept and hope for the best.' (Consumer 11)*

There are other cases, too, in which consumers do not go through a formal and conscious evaluation of what services to adopt and from which service provider. This is because of the complexity of the offerings as well as consumers' feelings of self-efficacy in comparing these services:

> *'I didn't know how to use it, I didn't know how to use the backup on the iCloud, it just comes with the device. Then when I wanted to buy larger data storage I went to a few different places, like I rang Optus, I rang Telstra because my iPad is with Telstra, and they were just so*

much more expensive. It was like about $80 a month for Telstra to have 25 gig, it was like $30 a month for Optus but then I would have had to change my service provider for the internet account for the iPad as well, and it just became really messy and confusing.' (Consumer 26)

The non-negotiability of standard contracts as well as the difficulty in understanding the terms of service is leading to a 'click-through behaviour' whereby consumers do not read the terms and simply click the 'agree' button to complete the registration process without awareness of what is written in the terms. A comparison of the terms of services of a sample of personal cloud services is set out in Table 5. The comparison shows that although some cloud service providers undertake to make the necessary backups (Hon, Millard & Walden 2012), none of them warrant data integrity, or accept liability for data loss. Service level standards are lacking, which makes it difficult for consumers to compare different services. Consumers need to develop a strategy on the type of data to put in their personal cloud as different providers have different policies on the use of the data.

Table 5 Comparison of personal cloud terms of services

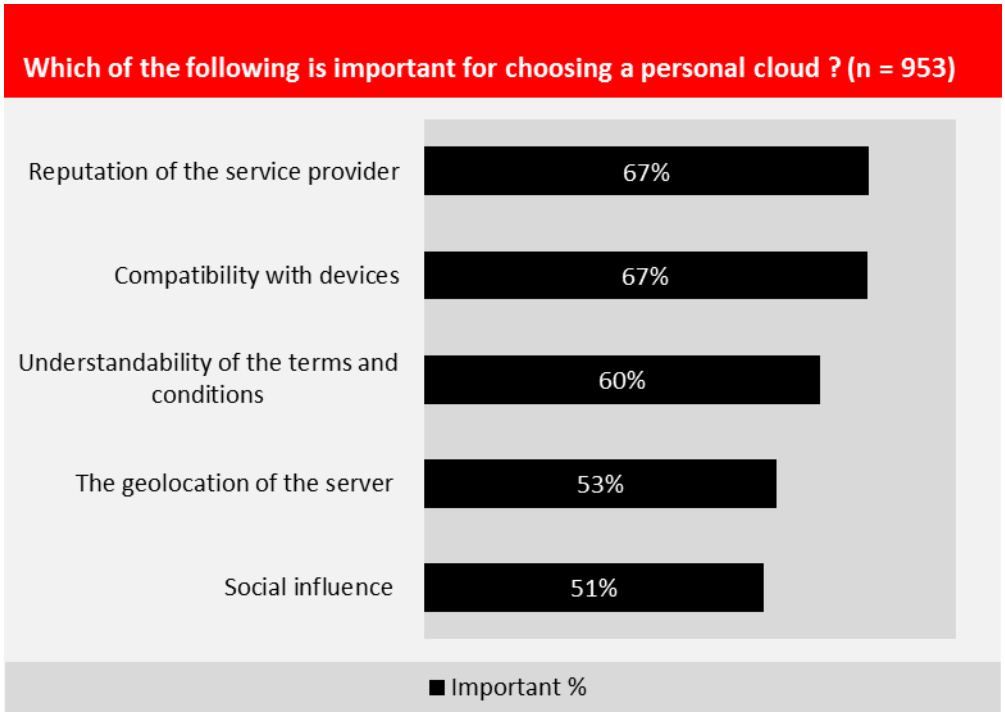
Criteria	Evernote	Dropbox	Google Drive	iCloud	GoPC	Onexus	Meeco	Cloud Drive	OneDrive	Box	T-Cloud
Which law governs the contract?	USA, Canada, Brazil, Switzerland	San Francisco, USA	California, USA	Santa Clara County, USA	User & GoPC domicile	Western Australia, Australia	New South Wales, Australia	Federal Arbitration Act, USA	Australian Consumer Law	Santa Clara County, State of California, USA	Australian State Law
Privacy certification	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	Not stated	TRUSTe	Not stated
What data are collected from you?	Name, email, address, IP	Name, email, contact, IP, address, device info, usage	Name, email, phone, credit card	Name, address, phone, email, credit card	Name, credit card, date, time, IP, browser, OS	Name, email, phone, credit card, IP, browser	Name, age, gender, email, browser, history ,language and geolocation	Name, phone, address, IP, photo, email, geolocation, browsing history	Email	Name, email, photo, address, phone, employer, job	Name, email, birthday, job, address, phone, driver's licence
Who uses data collected from you?	Evernote	Dropbox, law enforcement agency	Google, affiliate, law enforcement agency	Apple, law enforcement agency	GoPC, contractors, law enforcement agency	Not disclosed	MailChimp, Zendesk	Starbucks, AT&T,Sprint OfficeMax, , Verizon, T-Mobile, J&R Electronics, Eddie Bauer, Northern Tool	Microsoft, affiliate	MediaMath, Taboola, 33 Across, AppNexus, Google AdSense, Bizo	Telstra, contractor, affiliate, law enforcement agency
Security (data transfer and storage)	Unknown	Encrypted 256-bit AES	SSL encrypted 128-bit AES	TLS encrypted 128/256-bit AES	Encrypted 128-bit	Unknown	Unknown	SSL encrypted	SSL encrypted	SSL encrypted 256-bit AES	Unknown
How soon to inform of data breach	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed
Data retention after you delete	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed
Data recovery procedures 'safe haven'	Not stated	EU-US and Swiss-US Safe Harbor	EU-US. and Swiss-US Safe Harbor	US Department of Commerce	Must purchase a DRP plan	Not stated	Not stated	Not stated	Not stated	EU-US and Swiss-US Safe Harbor	Not stated
If you infringe copyright	30-day notice before suspension	Account suspended	Account suspended	Account suspended	Account suspended	Account suspended for repeat infringer	Not stated	Account restricted, suspended or terminated	Access limited or disabled, or account terminated	Content disabled or removed, or account terminated	Content disabled/ removed, or account terminated
Service warranty	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	None	Not disclosed
Compensation for data loss	Not disclosed	None	Limited to paid service	None	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not disclosed

Criteria for Choosing a Personal Cloud

The reputation of the service provider (67%) and the compatibility (67%) of the cloud service with consumers' devices were the two most important considerations for choosing a personal cloud (see Figure 8). Different countries have different data protection and privacy protocols. There is a push for cloud service providers to be transparent about the geolocation of their data centre and the applicable jurisdiction. Nevertheless, not all consumers realise that the geolocation of a cloud server determines the applicable legal jurisdiction. Thus, while 67% of the 953 consumers rated device compatibility as an important criterion for choosing a personal cloud, only 53% rated the geolocation of the server as an important consideration.

Figure 8

Consumers' criteria for choosing a personal cloud



Personal Cloud Precautions

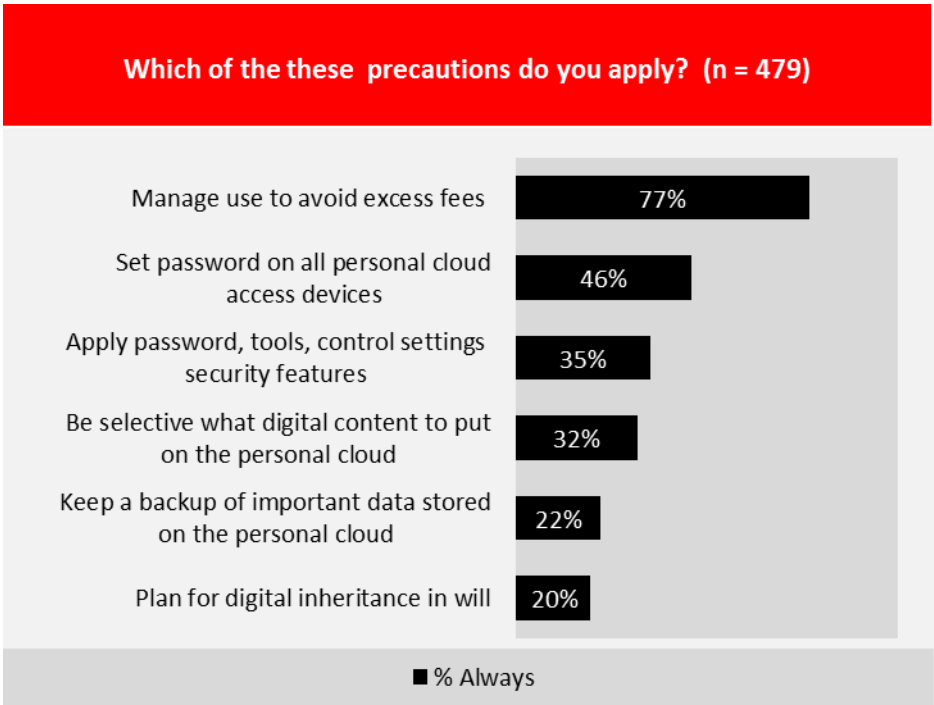
Data security and privacy both during transmission and on the cloud are significant concerns for most consumers. Despite consumers' expectations of reassurance from regulatory agencies as well as service providers that their data is in safe hands, most consumers were not taking personal precautions to secure their personal cloud use (see Figure 9). Seventy-seven per cent identified that they were managing their use to avoid excess fees. As a result, in the past two years, 23% of consumers had to pay excess fees at least once because they had exceeded the free allowance or paid subscription limits of their personal cloud. Younger (18–25) consumers were four times more likely than older (>56) consumers, males were two times more likely than female consumers and consumers earning more than $180,000 were four times more likely than those earning less than $19,000 to incur excess fees.

Even basic precautions such as setting the password of tablets, mobiles and personal computers and activating the security features of cloud services were always used by only 46% and 35% of

consumers respectively. Moreover, only less than 25% backed up their data and 20% had drawn up a plan for inheritance. Paradoxically enough, younger people were more likely to have a digital inheritance plan than older people. Males were twice more likely to have planned for digital inheritance than females.

Figure 9

Personal precautions for using a personal cloud



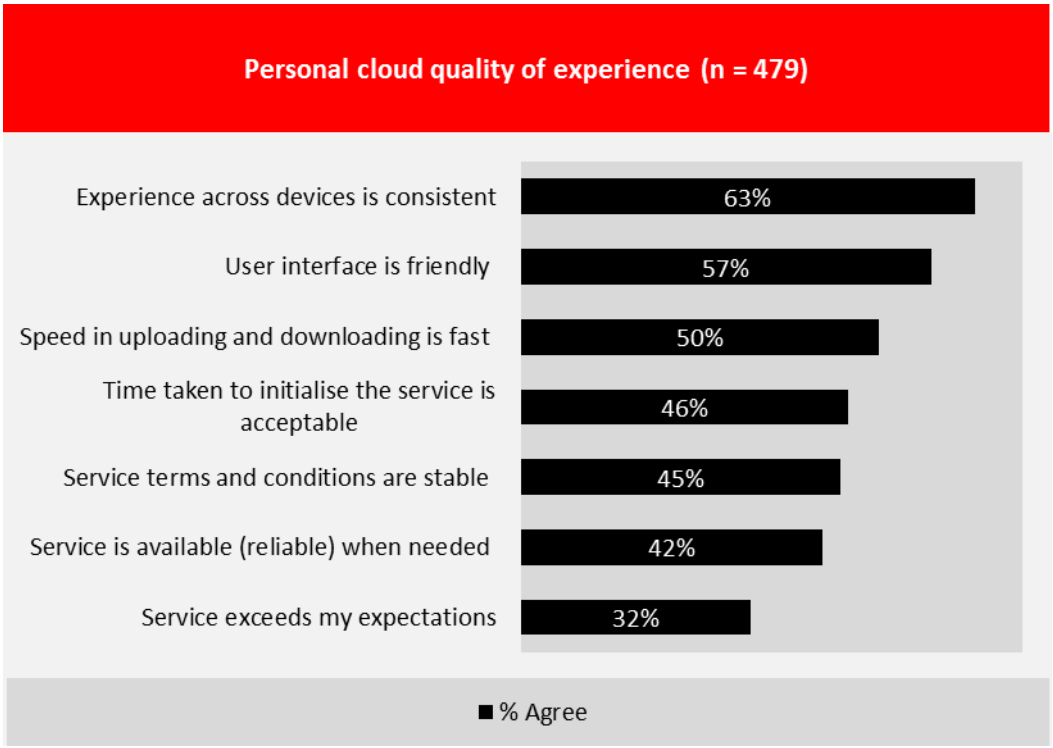
Personal Cloud Quality of Experience

The availability, accessibility and compatibility of personal clouds are important to consumers' quality of experience. Nevertheless, there is a concern that service providers may not give as much attention to personal cloud service as they do to the corporate cloud environment. We asked the 479 users to evaluate their quality of experience by reflecting on the personal clouds that they frequently used (see Figure 10):

- Only two out of three consumers reported that multi-device file synchronisation of personal clouds was consistent.
- For 43% of consumers, the user interface of personal clouds was unfriendly. Women were more likely to find the user interface unfriendly than men. However, 56% of 18–35 year olds and 43% of the above 56 years group found the user interface friendly.
- The speed of uploading and downloading files was perceived to be fast by half of the consumers and there was no noticeable difference due to consumers' geographical location.
- Most consumers believed that the application initialisation delay was not acceptable.
- The majority of consumers had experienced frequently changing service terms and conditions, which might be one of the reasons why very few of them read them.
- Forty-two per cent of consumers reported that personal clouds are reliable, that is, they are available when they are needed. Only 36% of consumers living in rural areas had had reliable experience.

- Overall, only 36% consumers agreed that the personal clouds they frequently used exceeded their service level expectations.

Figure 10 Quality of experience

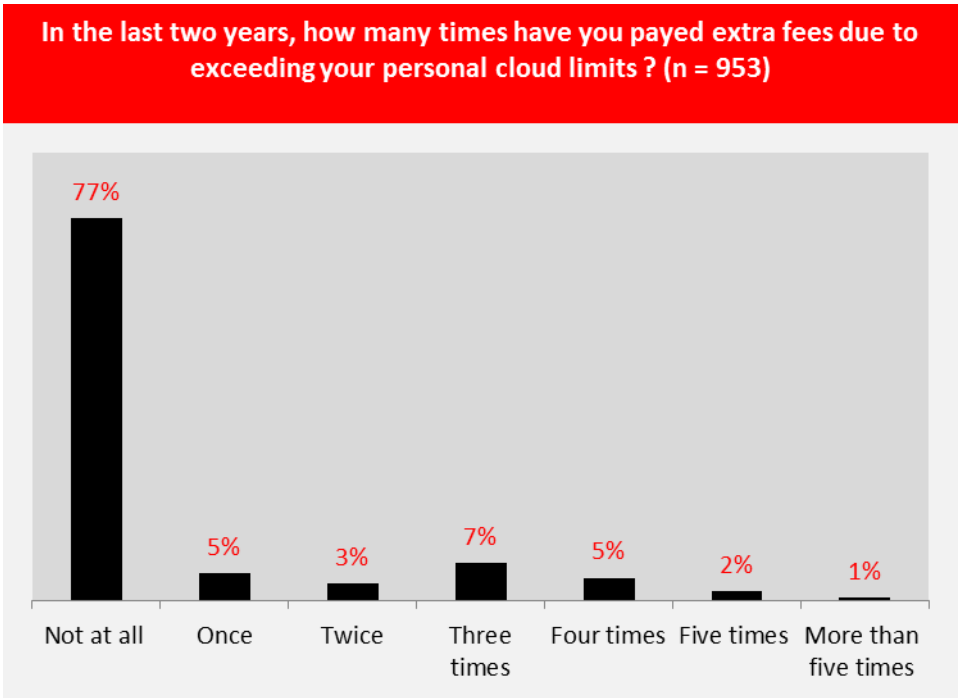


Personal Cloud and Communications Consumption

In the past two years, 23% of consumers had to pay excess fees at least once because they exceeded the free allowance or paid subscription limits of their personal cloud (see Figure 11). Younger (18–25) consumers were four times more likely than older (>56) consumers, males were two times more likely than female consumers and consumers earning more than $180,000 were four times more likely than those earning less than $19,000 to incur excess fees.

Figure 11

Extra fees due to exceeding personal cloud limits

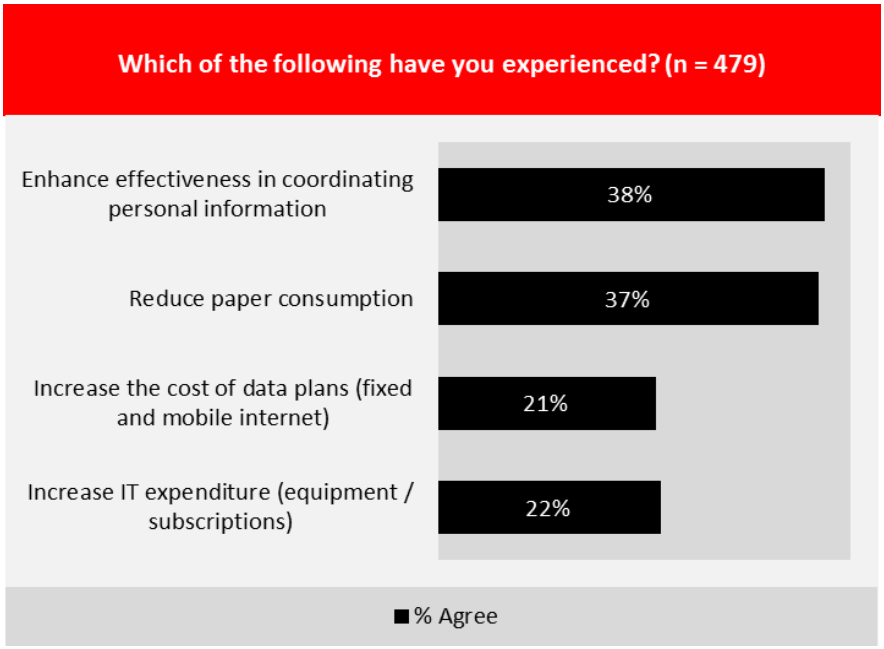


For one out of five consumers (see Figure 12), their use of the personal cloud, rather than reducing their IT expenditure, had indeed resulted in increasing their IT expenditure through acquiring new devices and upgrading data plans:

- Consumers in the age group 26–45 were four times more likely than those above 65 years, and male consumers were twice more likely than female consumers to increase their IT and data plan expenditure.
- About 20–25% of consumers earning less than $80,000 reported having increased their IT and data plan expenditure to use their personal cloud.
- Interestingly, while 75% of consumers with primary education reported increased IT expenditure due to their personal cloud, only less than 5% incurred excess fees because they had exceeded their limits in the past three years. Instead, 23% and 36% of consumers with first and master's degrees respectively had to pay excess fees at least once in the past three years for exceeding their limits.
- The majority of consumers had yet to reduce paper consumption (37%) and enhance the effectiveness of managing personal information (38%) through using a personal cloud. Nevertheless, more than 50% of the consumers with a higher degree (master's or PhD) reported that their personal cloud use had increased their effectiveness in managing personal information.

Figure 12

Personal cloud consequences

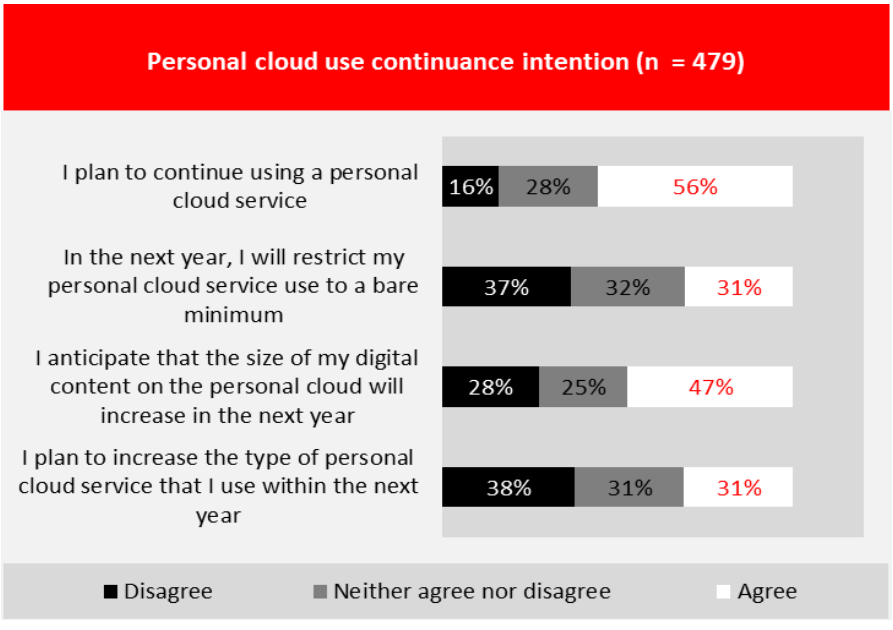


Future Intentions

Current users' intentions to continue using personal clouds were mixed (see Figure 13): 56% were certain that they would continue using a cloud service within the next one year, 47% anticipated an increase in the volume of digital content on the cloud and 31% intended to diversify the type of cloud service they used within a year. However, 31% intended to limit their cloud usage. There was a high and statistically significant correlation between the consumers' personal cloud self-efficacy and belief that a personal cloud enhances performance and the intention to continue using the cloud.

Figure 13

Users' personal cloud use continuance intention

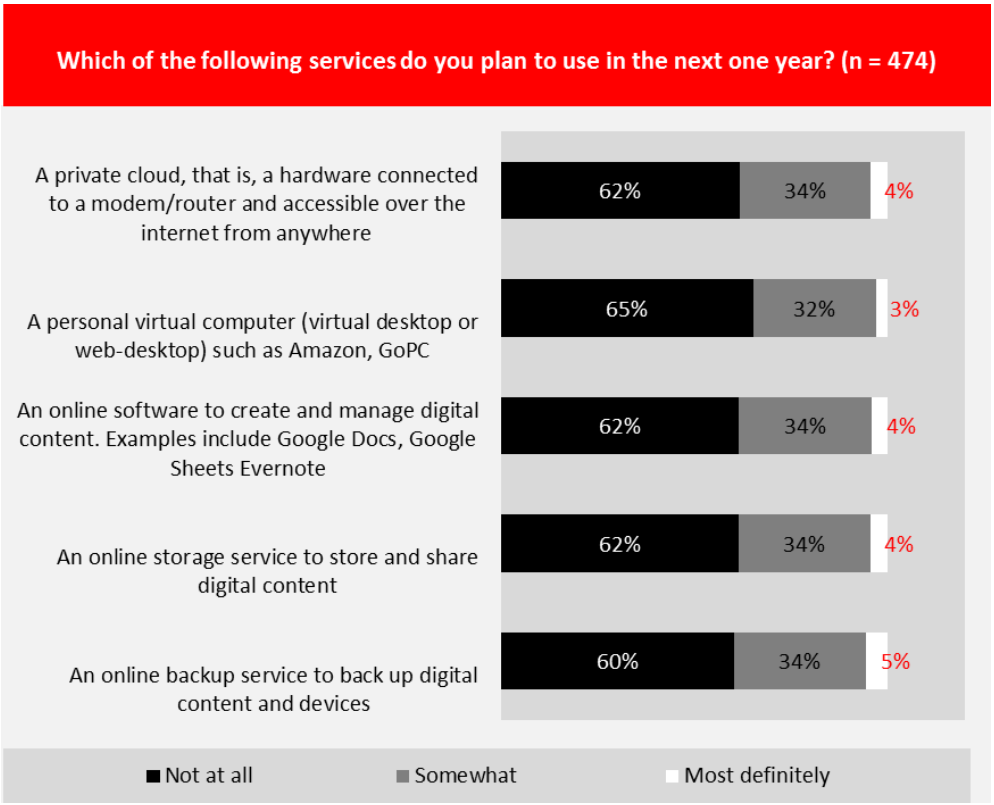


When non-users were asked whether they intended to use the five different types of personal cloud services t one year, in each case, more than half of the respondents answered that they had no intention of using such a service, and in each case, only about 4% most definitely planned to adopt some form of personal cloud service (see Figure 14).

Older people were less likely to adopt personal cloud services in the future. The percentage of people over the age of 65 that had no intention of using a personal cloud was between 75% and 77% for each of the five types of personal cloud service, compared with 28–31% for 18–25 year olds. Neither education nor gender seems to have had any influence on non-users' plans to adopt personal cloud services. People with incomes between $19,201 and $37,000 were most likely to consider using personal cloud services in the future.

Figure 14

Non-users' intentions to adopt a personal cloud



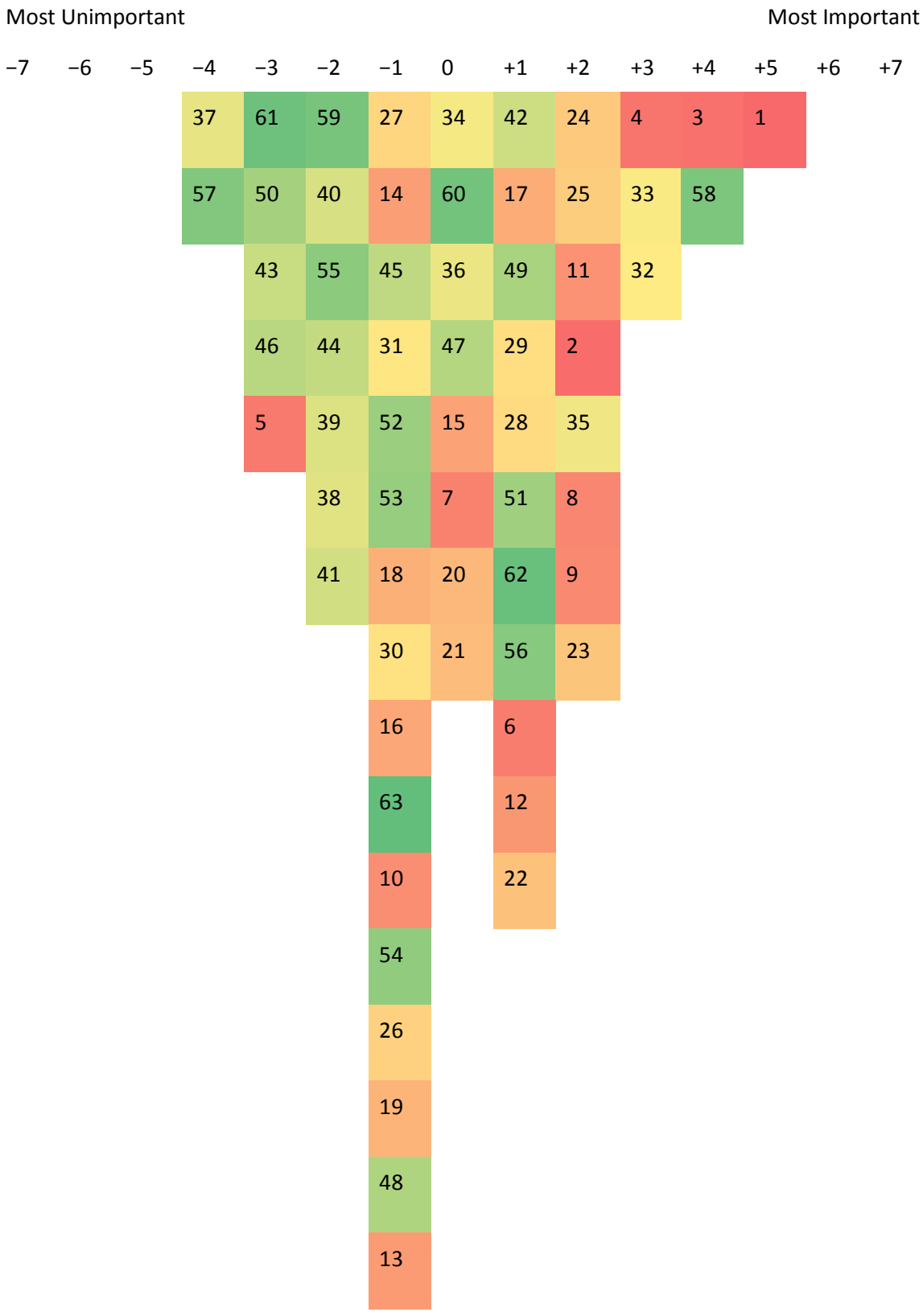
Most and Least Important Personal Cloud Issues

As indicated in the research methods section, to identify the most important and unimportant personal cloud issues, we conducted 26 structured Q-method interviews (Thomas & Watson 2002). Consumers were asked to sort the importance of 63 personal cloud statements (see Table 6) using a 15-point 'Q-scale' ranging from –7 (most unimportant) through zero to +7 (most important). The average score of each item across the 26 interviews was calculated. The result is depicted in Figure 15.

Table 6 Q-method interview items

1. Privacy of my data
2. Privacy of my metadata
3. Security of my data at the cloud servers
4. Security of my data during transmission
5. Geolocations of the cloud servers are clear to me
6. Using personal cloud service to back up my computer
7. Using personal cloud service to back up my mobile device
8. Using personal cloud service to store my personal data
9. Using personal cloud service to store my work-related data
10. Using personal cloud service to share/stream media
11. Using personal cloud service to synchronise data across computers and devices
12. Using personal cloud service to improve my productivity
13. Using personal cloud service to connect with my family
14. Using personal cloud service to connect with my friends
15. Using personal cloud service to connect with my colleagues
16. Using personal cloud service to connect with other professionals
17. Personal cloud services that provide multiple utilities (e.g. storing data, synchronising data, sharing data, social networking)
18. Scalability of personal cloud services (e.g. freemium, paid 50 GB and paid 100 GB)
19. Ability to bundle personal cloud services with others (e.g. home phones, mobile phones and internet access)
20. Costs of personal cloud services remain free
21. Indirect costs (e.g. upgrading internet plans, using up-to-date devices, and buying new software) for using personal cloud services are minimal
22. Sizes of online spaces that I can use to store data
23. Speed in synchronising files across computers and devices
24. Choices of movement (e.g. easy to access data from different types of devices)
25. Service reliability (i.e. uptime–downtime rate)
26. Maturity of personal cloud products/services
27. Personal cloud providers have commitment to extend/upgrade current system functionalities
28. Integration of personal cloud services with software that I am using
29. Compatibility across platforms (e.g. Windows, Mac OS X, Android, iOS)
30. Functionalities that reduce bandwidth usage such as local synchronisation (i.e. LAN sync) or online browsing (i.e. no need to download files first)
31. Functionalities that allow me to create my own personal cloud service (i.e. do-it-yourself)
32. Settings that allow me to control how my data will be accessed or shared
33. Ability to recover my lost data
34. Data portability (e.g. bring your own data to another provider)
35. Trust in personal cloud service providers
36. Reputation of personal cloud service providers
37. Personal cloud services that I use must be offered by large firms
38. Technologies offered by personal cloud service providers enhance eco-sustainability
39. The number of my family members and friends who use the same cloud service
40. The number of my colleagues who use the same personal cloud service
41. The number of people who use the same personal cloud service
42. Personal cloud service providers are trustworthy
43. Websites that compare personal cloud plans and providers before signing up
44. Websites that teach me how to protect myself while using personal cloud services
45. Easy-to-understand terms of service
46. Negotiable terms of service
47. How personal cloud service provider will harvest and use my data/metadata is clear to me
48. Better services based on my personal data/metadata
49. Easy-to-use interface across multiple devices
50. Accessibility of personal cloud services for people with disabilities or special needs
51. Interface that allows me to manage privacy of my data/metadata easily
52. Explanation of how personal cloud services are configured and delivered is clear to me
53. Being informed when terms of service are updated
54. Quality of after-sales services
55. Quality of dispute resolution process
56. Accountability of personal cloud service providers when my data were lost/stolen
57. Ability to use my personal data as a commodity or currency
58. I remain the owner of my data
59. Easy to get out of the contract
60. Procedures to handle my data after I have deleted them
61. Procedures to handle my data after death
62. Personal cloud providers comply with international security standards
63. Australian laws and standards apply to personal cloud providers

Figure 15 Distribution of most important and unimportant personal cloud issues



Most important issues

Data security and privacy both during transmission and on the cloud topped the list of important issues. However, there were some contradictions between the level of concerns for privacy and the actual behaviour of many consumers, as noted by one the government agency managers interviewed:

> *'It's funny, I've seen other studies too just about people's perception of privacy, and everyone is concerned about privacy, yet our behaviour suggests, in the online world, that we're happily trading it off every time we do something on Facebook. So we do these studies, and privacy related concerns come up again and again, but when you actually look at what people are doing, it actually suggests the opposite, that they are behaving in a way that doesn't indicate that they have particular concerns about privacy.' (Regulator #1)*

The second batch of important issues reflects the motivation for using a personal cloud. The drivers were the utility of the personal cloud to manage the blurring of work and personal use of devices and services; the growing volume, variety and velocity of consumers' generated digital content and the need to easily access, share and stream that content anywhere, anytime; and consumers' use of multiple computing and communication devices such as smartphones, personal computers and other smart devices that should provide a synchronised access to digital content.

The functional affordance and operational performance of personal clouds that affect consumers' choice and quality of personal cloud experience was the third category of important issues. These include compatibility across platforms, easy-to-use interface across multiple devices and content, integration of the personal cloud with software that consumers use, data portability, procedures to handle lost data and the size of cloud storage and provider reputation.

Least important issues

Regarding the most unimportant issues, the size of the service provider was the most unimportant issue for the Q-interview participants. This is somewhat inconsistent with the focus group and survey participants, who tended to choose global personal cloud providers such as Dropbox, Google and Apple that offer a range of bundled services over Australian personal cloud providers that offer niche services.

Data sovereignty, which surrounds the ownership and control of digital data and the protections that apply to it, is complex in the context of the personal cloud, where data is stored across global jurisdictions. Nonetheless, the Q-interview findings reinforce the findings from the focus group and survey that consumers are not as aware as they need to be about the true value of their personal data. Consumers understood that providers offered 'free' services to them because providers often earned revenue from advertising to them. They also had some insight around how personal cloud providers sold on their data to other organisations; however, they did not necessarily understand the true value of their data and their potential to be used as an asset, commodity or currency.

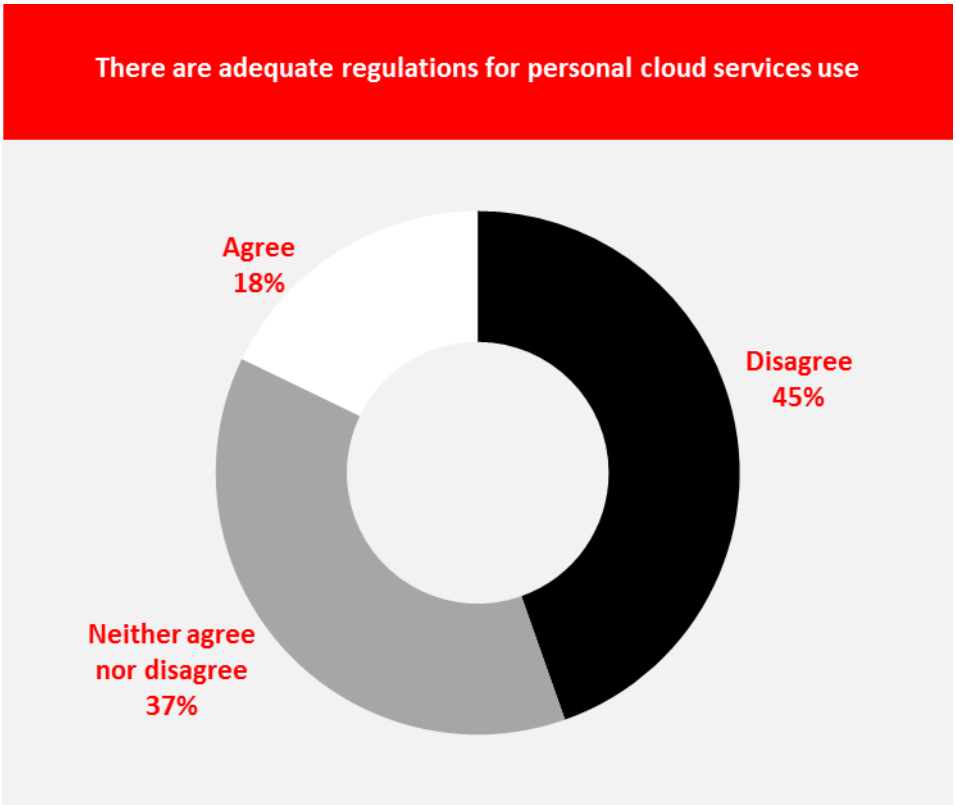
For some consumers, the choices made by family and social ties as well as their professional life contributed to their personal cloud service and provider choice; however, for Q-interview participants, this was not the case. The issues related to consumers' decisions to discontinue a

personal cloud service, such as ease of exit, cost of exit, digital footprint and inheritance, were not considered that important, perhaps reflecting the extent of awareness about these issues.

Evaluation of Consumer Protection and Privacy Codes

Consumers require reassurance from both regulatory agencies and service providers that their data are in safe hands. For example, legislation that requires firms to inform customers of data breaches within a short period of time to build consumers' confidence and reduce the perceived vulnerability associated with the use of a personal cloud would be valuable. The survey finding (see Figure 16) demonstrates that only 18% of the consumers agreed that the current regulations were adequate to cater for cloud use.

Figure 16 **Consumers' perception of the adequacy of current regulations**



Therefore, we evaluated existing consumer protection and privacy codes in view of the experience and expectations of consumers of personal cloud services.

Main regulatory instruments for personal cloud services

According to the ACMA (2013: p.3):

> 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.

Thus, personal cloud service providers are not clearly covered under the two service types, that is, carriers and carriage services, defined in the *Telecommunications Act* (ACMA 2013). However, they might fall under the obligation of content service providers referred to in the *Telecommunications Act*, which includes any 'online services'. Nevertheless, the majority of the content service provider rules refer to broadcasting and hosting services and the extent to which the obligations are applicable to the different types of personal clouds is ambiguous.

Geolocation

Consumers use cloud services from both Australian and overseas providers. There is a need for clarity as to which Australian regulations apply and the extent of protection or regulation that the ACL will ordinarily apply. There may be practical challenges in enforcing a regulation, for example, if the provider is located overseas.

Personal cloud security

As per the *Telecommunications Act,* s. [13], carriers and carriage service providers must protect 'the confidentiality of communications'. The *Privacy Act 1988* further implies that cloud service providers that collect, hold and store personal information must be responsible for data security. However, both the *Telecommunications (Interception and Access) Act 1979* and the *Privacy Act* (Australian Privacy Principles 6, 12) include exceptions that make it possible, in the case of intercepting and accessing information, to execute a warrant issued by an Australian law or court and under extreme emergency situations. This means consumers that are concerned about personal cloud security and digital surveillance can be reassured that, unless a warrant is issued, existing regulations provide sufficient protection to the confidentiality of consumers' data during transmission and storage.

Privacy of data in personal clouds

The *Privacy Act 1988*, its accompanying Australian Privacy Principles and various state privacy Acts regulate the handling of personal data and impose obligations about security. The *Privacy Act,* s. [b 79], defines personal information as:

> 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.

The Act treats the obligation of data controllers, such as consumers of personal cloud services, differently from the processors of data, that is, providers of a personal cloud (DOC 2014). The Act defines 13 Australian Privacy Principles that offer comprehensive coverage of personal cloud–related privacy issues such as collection of personal data, data ownership, jurisdictional coverage and differences; cross-border disclosure of personal information; and data loss, storage and deletion.

Nevertheless, although mandatory data breach notification has been identified as warranting consideration in future law reform, the Act currently does not specify the obligation of personal cloud service providers to inform consumers in case of a data breach.

In addition, personal cloud providers notify consumers that they collect personal information. It is important to monitor whether the personal information that personal cloud providers (particularly

overseas providers) collect meets the definition of personal information under the *Privacy Act 1988* and the method of data collection and its use comply with the Australian Privacy Principles.

Data retention

The Australian government requires the telecommunication industry to retain metadata for two years for national security reasons. The government defines metadata as 'information about a communication (the who, when, where and how)—not the content or substance of a communication (the what)' (Australian Government 2015). For internet activity, metadata is information such as an email address and when it was sent—not the subject line of an email or its content. The definition excludes 'a person's web-browsing history or any data that may amount to a person's web-browsing history' (Australian Government 2015).

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* does not specifically address data stored in a personal cloud. It is also not clear whether personal cloud providers fall under 'the telecommunications industry' as they are not strictly providing 'carriers and carriage services'. The exclusion of a person's web-browsing history from the *Data Retention Act* appears to exclude traffic to and from cloud services. However, the sharing of digital content through personal clouds can be considered an online communication and could be subject to the enforcement of the Act.

Law enforcement agencies can seek authorisation under the *Telecommunications Interception and Access Act*, the *Cybercrime Act*, the *Crimes Act* and the *Criminal Code Act* to access both data and metadata for criminal and national security investigations. Despite consumer fears, particularly around warrantless data collection, the *Data Retention Act* does not provide additional or new powers to agencies. Existing criminal laws provide law enforcement agencies with appropriate warrants the power to search, confiscate and recover data from computers, electronic devices and other digital sources. These powers as well as those related to investigating cyber and computer crimes are applicable to personal clouds.

Premium pricing

Most of the consumers that we talked to were using and intended to continue using free cloud services. Only a few were opting for premium services. In the current environment, vendors are free to set their own prices as there is no regulation to govern information and communications technology (ICT) services pricing in Australia (DOC 2014). Potential issues may arise if personal cloud services lack interoperability and price rises make it unaffordable for consumers to access their content, information or applications from a particular provider. Nonetheless, the ACCC is responsible for ensuring vendor compliance with Australian competition, fair trading and consumer protection laws such as the *Australian Consumer Law 2010*. This offers some protection for consumers using personal cloud services in regard to issues such as unfair market practices.

Interoperability

Personal cloud services are not fully interoperable, which creates some difficulty (inconvenience) in moving data across different service platforms. The *Competition and Consumer Act* provides some

protection against vendors that attempt to lock in consumers by making switching from one personal cloud service to another either impossible or high cost.

Copyright

Two of the common elements in personal cloud terms of service are 'acceptable use' and 'copyright infringement'. Vendors reserve the right to delete content and/or suspend or cancel consumers' accounts (with or without notification) if they suspect that consumers are infringing copyrights. In Australia, the *Copyright Act 1968* primarily governs copyright issues. According to the Department of Communications (2014, p. 15), '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 particular, there are grey areas and uncertainties about whether existing copyright exceptions covering fair dealing, format and time shifting are applicable to personal cloud use. The Australian Law Reform Commission has investigated the adequacy of Australian copyright law for cloud services and tabled 30 recommendations for reform in Parliament in 2014. Further, the Copyright Amendment (Online Infringement) Bill 2015, which would enable copyright owners to apply to the Federal Court to oblige carriage service providers to block overseas websites that infringe copyright, may affect consumers the rely on cloud services that have been blocked, without their knowledge.

Terms of service

Personal cloud services are provided under the standard form of contracts, in which the terms and conditions are on a 'take it or leave it basis'. The *Australian Consumer Law 2010* protect consumers from unfair contract terms in standard contracts:

> 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.

Personal cloud contracts favour service providers as they can change the performance of the cloud services, such as in size, speed and file delivery mechanisms, without consumers' consent. This is one area that needs to be examined more closely to ensure that personal cloud contracts are consistent with the ACL. The issue is further complicated by the fact that most consumers use personal cloud services provided by international companies and there may be practical challenges in enforcing the relevant Australian laws when the provider is based overseas.

Service warranties

Personal cloud providers do not provide warranties as to the availability and performance of cloud services. This means consumers could be subject to data loss if a service provider discontinues (or disrupts) its services for various reasons. However, the ACL stipulates consumer guarantees that cannot be excluded by service contracts. In addition, based on the *Privacy Act 1988*, cloud providers have certain obligations in relation to data protection. There is potentially a variation between the service providers' terms and applicable Australian laws whereby contract terms may limit the liability of a guarantee. Further, 'currently under Australian law, there is limited legislative protection for return of data in the event that a cloud service is shut down' (DOC 2014, p.45).

Consumer complaints and dispute resolution

Personal cloud (such as storage as a service, backup as a service, software as a service and computing as a service) providers do not strictly fall under the *Telecommunications Act*. It is unclear whether the Telecommunications Industry Ombudsman (TIO), which focuses on the supply of landline, mobile and internet communications, can provide dispute resolution services to personal cloud consumers. It is also important to investigate whether the Telecommunications Consumer Protection Code (TCP) provides adequate coverage of the privacy, billing, customer transfer and complaint-handling issues of personal cloud services. This creates uncertainties because consumers might not clearly know to whom to complain when personal cloud services fail to meet contractual expectations.

CONCLUSIONS

The Personal Cloud is Not Truly Personal in Its Current Form

The current provision of the personal cloud is not customisable or configurable to consumers' specific needs. Instead, it is supplied on a one size fits all basis. This is typically evidenced in the terms and conditions because consumers are only given the option of accepting or not accepting the offer. Consumers are concerned that they cannot opt out from some of the conditions without losing the part of the service that they would like to keep. Consumers that are using either a Google or an Apple service do not actually hold the encryption keys for that cloud. They do not control that cloud and that cloud is a section of a bigger space. Therefore, the current models of the personal cloud are far from the vision of the personal cloud articulated by Ernst (2012), where users have totally autonomy to:

> choose and remove the apps they run on their personal cloud … control who does and does not get access to the data … process data created with one app with another in a similar way as files on a PC may be opened by apps from a different vendor … set the terms of use themselves … move the personal cloud from one host / infrastructure / hosting provider to another if needed.

To Cloud or Not to Cloud

The consumers and other stakeholders we interviewed recognised many benefits of the personal cloud, such as the convenience of sharing, collaboration, connectedness, accessibility, trusted virtual backup and extending the storage capacity of mobile devices for consumers. Nonetheless, they identified a number of issues and concerns. Some, such as privacy and security, have been previously reported in the literature. Others (value for data, surveillance) are additional insights. The identified issues will not deter consumers from using the cloud, as most believe that with a proliferation of mobile devices, to use or not to use a personal cloud is no longer a real choice. Instead, these issues improve or affect the quality of consumers' experience and the extent of assimilation of the personal cloud in their personal and social life.

Consolidation of the Personal Cloud Market

Apple, Dropbox, Google and Microsoft dominate the personal cloud market, together representing 86% of personal cloud services reported in the survey. These companies target multiple dimensions of the personal cloud market alongside smaller providers that are trying to capture the market with more 'vertically oriented and dedicated offerings' (e.g. streaming services accessible from particular platforms or devices) (Gartner 2012). It is anticipated that personal cloud competition among cloud service providers will grow in three different directions (Gartner 2012). This first direction is mobility and location, through which contextually based devices and platforms will provide consumers with relevant information, at the relevant location, using their favourite devices. The second is platform independence, through which platforms will be judged based on the availability of the core personal cloud services rather than solely by number of applications. The third is seamless synchronisation: at

present, no cloud service provider claims to offer a solution for synchronisation of all types of consumer data.

Data Value Asymmetry

Most cloud services use a 'freemium' model. Consumers appreciate the seemingly free service but 'obviously, everyone knows there's no such thing as a free lunch' (Consumer 18). Consumers' data are becoming increasingly valuable to companies that offer free personal cloud services. That is because data can be an asset, a commodity and a currency. As an asset, data can be traded in such a way that when consumers give away their data it allows others to gain utility and value out of it. However, most consumers are not benefiting from the true value of their data and there are not many cloud providers with such value propositions.

One Size Does Not Fit All

Although consumers of the personal cloud share some common concerns, based on our analysis (see Appendices E, F and G for detailed statistical analyses), there could be as many as six different categories of personal cloud consumers. These categories of consumers differ sufficiently from one another in terms of the emphasis placed on issues affecting their awareness, behaviour, practice and experience. We name these groups as risk averters, productivity maximisers, social users, hesitators, vault seekers and usability explorers.

Risk averters

Risk averters are sceptical and highly concerned about the potential harmful consequences of the personal cloud. They use personal cloud services to store, back up and synchronise their personal data across devices. They prioritise mitigating risks from using personal cloud services as the most important. As a result, they are very reluctant to use personal cloud services to connect to their families, friends, colleagues and other professionals. They give high priority to security measures that are implemented both during transactions and data storage and that these security measures meet international standards. They are especially concerned about privacy and ownership of their data and metadata, how the data and metadata will be used by service providers and to what extent they will be able to control who will have access to their data. As a result, they do not view the practice of providing additional personal information to obtain better services or using their data as a commodity as important. In choosing a cloud service, they want to ensure that the provider has good dispute resolution and lost data recovery procedures and provides reliable services in terms of synchronisation speed. Subsequently, they sometimes investigate which providers they should use before signing up or opening an account and can independently decide which service to use without being influenced by families, friends, colleagues or the number of consumers using the same service.

Productivity maximisers

Productivity maximisers use the personal cloud to improve their personal productivity by storing, backing up, synchronising and sharing their personal and work data across multiple devices and collaborating with their families, friends, colleagues and other professionals. Although privacy of data and metadata is still important to them, they are willing to trade off that for better services such as synchronisation speed, easy-to-use interface and compatibility across devices and platforms.

Their concern for security during data transmission does not extend to verifying whether the implemented security meets international standards. They also value the ability to recover lost data but at a relatively lower level than the personal cloud risk averter group. When deciding which personal cloud services to use, this group of consumers is influenced more by the perceived productivity gains from using a service and by what their network of collaborators use than by the size and reputation of service providers. This category of consumers, as long as they believe that cloud services improve their productivity, is not particularly concerned about how cloud services are configured and delivered, where cloud servers are located, how data and metadata will be used by service providers, whether they will be informed when terms of services are changed, who will be held liable when data are lost or stolen, how disputes will be resolved, or how their data will be handled after their death.

Social users

Social users use the personal cloud to advance their social networking and prefer streaming platform services. As long as a personal cloud is perceived to deliver their social networking needs, they may be willing to pay for it and upgrade their internet plans or devices. Their choice of personal cloud is influenced by their family and friends, the quality of interface, not necessarily across devices or platforms, and the reputation of providers rather than self-evaluation of the risks and benefits of a service. For this group, a provider's reputation mitigates any concern about the maturity and scalability of services, integration of services with other software and future extension of functionalities. Since social users connect themselves to many people and share a great deal of digital content, they are quite concerned about the privacy, security, ownership and recoverability of data and metadata. As a result, they continuously search for ways to protect their privacy rather than expecting laws to be imposed on providers when problems arise.

Cloud hesitators

Cloud hesitators stand out because of their low degree of innovativeness in using the personal cloud. They use the personal cloud for data storage and avoid the social aspects of the personal cloud. Their use of the personal cloud is quite limited because of their privacy, security and user interface concerns. They are very reluctant to trade off their data and metadata as forms of commodity to obtain better services. For this group, perceived personal trust is a dominating factor in choosing a cloud service. Nevertheless, families, friends and other people using a particular service, the size of the firm, or the provider's reputation rarely contribute to the formation of their trust. Instead, cloud hesitators seek reassurance on how to protect themselves by doing their own research on terms of services and contracts, configuration and delivery of personal cloud services, and procedures for handling data after deletion or death. The enforcement of Australian laws and the clarity of regulations that define the extent of providers' liability are other important sources to build their trust. Somewhat paradoxically, this group of respondents do not seem to realise that the geolocation of a cloud server determines the applicable legal jurisdiction. It will take some time before personal cloud hesitators are convinced they should diversify their personal cloud use (such as through bundled personal cloud offerings) or are willing to pay for premium services or upgrade data plans and change devices.

Vault seekers

A distinctive characteristic of vault seekers is that they predominantly use personal clouds to store work and personal data to avoid data loss. They strongly believe that personal cloud providers are trustworthy. Although they perceive that a personal cloud is a safe place to store their data, somewhat surprisingly, they do not use a personal cloud to back up their computers and mobile devices. They neither share the data with others nor believe that use of a personal cloud improves productivity. Personal cloud functionalities that reduce bandwidth usage such as local synchronisation (i.e. LAN sync) or online browsing (i.e. no need to download files first) are not perceived as important. They are also indifferent about data synchronisation, choices of movement, providers offering multiple utilities and bundled services. Instead, the privacy of data and metadata, data ownership, security of data on the cloud and the geolocations of cloud servers are important considerations. Although vault seekers are less likely to share their data with others, their choice of which cloud service to use is influenced more by their colleagues and the size of online spaces available to store data than by the size of the cloud provider or third party websites that compare personal cloud services. Although they do not seek to read and understand terms of services, they still want to be informed whenever there is an update in the terms. Because the data are work related, they have less concern about procedures for handling data after deletion or their death. Another characteristic of this group is a willingness to pay for premium cloud storage service but a desire to minimise indirect costs (e.g. upgrading internet plans, using up-to-date devices and buying new software) in using a personal cloud.

Cloud usability explorers

Cloud usability explorers are consumers that continuously explore personal cloud functionalities. A characteristic of consumers in this group is that, although they use a personal cloud to store work data, back up computers, synchronise files across devices and share files with their colleagues, they tend not to use a personal cloud to store personal data. Further, instead of privacy and security, consumers in this group focus heavily on the usability and functionality. Thus, multiple utility offers, accessibility, the size of online spaces, integration with other software, functions to reduce bandwidth usage, recovery of data lost, synchronisation speed, choices of movement, service reliability and future plans to extend service features are very important to them. Their choice of personal cloud is influenced by the maturity of services as well as the size and reputation of the provider. Families, friends and colleagues, and third party websites that compare cloud services have no or little influence when they are choosing a personal cloud service. Because these consumers prefer not to use a personal cloud for personal data, they do not see any value in websites that teach them how to protect their privacy while using a personal cloud. In addition, they do not consider the geolocations of cloud servers, data ownership, how service providers use data and metadata and procedures to handle data after deletion or death important factors that influence their personal cloud choice and use practice.

The Regulatory Environment for the Personal Cloud

Australian consumers are protected by a range of existing regulations and tools in their use of personal clouds. Based on our assessment, we did not find any particular regulation or legislation that was a real barrier to personal cloud services flourishing in Australia. Existing regulations and

tools, although not specific to personal clouds, are broad and flexible enough to cover most of the known consumer concerns. Consistent with the National Cloud Computing Strategy (DBCDE 2013) and the Department of Communications Regulatory Stocktake (DOC 2014) reports, new legislation specific to cloud computing and personal clouds may not be warranted. There are, however, a number of grey areas that create uncertainties when these regulations and tools are considered in the context of personal clouds. Key issues surround uncertainty as to how personal cloud services are classified in terms of existing legislation, geolocation of personal cloud services, the requirement of providers to inform consumers about data breaches, the use of private information collected by providers (particularly overseas providers), copyright, the consistency between personal cloud contracts and consumer law, and the extent to which agencies can provide dispute resolution relating to personal cloud services.

These grey areas may become clearer when existing legislation and tools are applied in practice. Further, government agencies such as the ACCC might further prioritise enforcement of the ACL by international personal cloud service providers. In the meantime, education and awareness programs for consumers are particularly important to complement existing consumer protection. This is consistent with the findings of the Australian Computer Society (ACS) following their extensive consultation with stakeholders regarding the need for a voluntary NCCP (ACS 2013a, 2013b). While there was largely a lack of support for such a protocol, education and awareness was seen as important given that existing legislation and consumer protection comes into play after perceived damage is suffered. Legislation and consumer protection do not provide guidance or information on prepurchase issues, set-up mechanisms, benefits, risks, costs or how to choose between suppliers. Delivery of such education and awareness campaigns would contribute to the fulfilment of the aims of the National Cloud Computing Strategy and benefit the consumers of personal cloud services (DBCDE 2013).

RECOMMENDATIONS

Recommendations for Consumers

Assess personal cloud readiness. The personal cloud requires a high-bandwidth internet connection with a decent data plan. This creates a high degree of dependency on the network, and consumers may be locked out of their digital content because of network disruptions. Consumers must evaluate the extent of their digital content, their demand for data upload or download, their mobility, and the quality and affordability of the internet connection available to them in order to choose a personal cloud service that best maximises their experience. If consumers do not have a high-bandwidth connection, data transfer will be sluggish and the cloud experience unappealing.

Caveat emptor. Consumers should consider their current and future needs for a personal cloud in choosing digital devices (e.g. mobile phones, tablets and computers) as, increasingly, cloud services are attached to their devices and result in an 'unintentional choice' of cloud providers. Australian consumers have a range of cloud services and providers from which to choose and they should weigh up the advantages and disadvantages offered by large well-known global brands versus small local Australian companies offering niche services.

Avoid click-through behaviour. Personal clouds are provided under standard contracts, which are regulated under the ACL. These contracts allow service providers to change the performance of their cloud services, such as in size, speed and file delivery mechanisms, without consumers' consent. Consumers need to avoid the 'click-through behaviour' whereby they do not read the terms and simply click the 'agree' button to complete the registration process without awareness of what is written in the terms. The consumer guide included in this report can assist to mitigate this issue by identifying the most common areas that consumers need to scrutinise in service contracts.

Apply personal precaution. Data security and privacy both during transmission and on the cloud are major concerns for most consumers. Despite consumers' expectations of reassurance from regulatory agencies as well as service providers that their data are in safe hands, most consumers are not taking personal precautions to secure their personal cloud use. These personal precautions include managing usage to avoid excess fees, checking the terms of service to ensure that their cloud provider has a third party (such as TRUSTe) certification or complies with known data-handling standards such as the US-EU-Switzerland Safe Harbor Framework, setting a strong password for tablets, mobiles and personal computers, activating the security features of cloud services, being selective about what digital data to keep in a personal cloud and keeping backup.

Plan for digital inheritance. The personal cloud increases consumers' digital content and elevates the need for planning who can access their online accounts after their death. The issues include who will inherit data, how to authenticate multiple accounts, how to respect the privacy of the dead and their correspondents, how to dispose of the digital footprint and who will own digital credentials. Consumers need to have an appropriate plan in their will for how their digital assets will be passed on after their death.

Recommendations for Personal Cloud Providers

Full service disclosure. The personal cloud space is emerging. Considering that some consumers do not have a full understanding of what they are using, what they are signing up for, where data end up, and their rights and obligations, there is an issue of the extent to which providers are providing a full product disclosure that satisfies existing laws in a form that is accessible to a wide range of consumers.

Cater for digital footprint and inheritance. When consumers can no longer use a service for reasons such as death, the way in which providers handle consumers' data is not entirely clear. The issues include who will inherit data, how to authenticate multiple accounts, how to respect the privacy of the dead and their correspondents, how to dispose of the digital footprint and who will own digital credentials. While some service providers do not specify a clear policy addressing these issues, others have clauses that restrict the 'right of survivorship and non-transferability'.

Improve quality of experience. Consumers are experiencing a number of inconveniences with personal clouds such as inconsistency in multi-device file synchronisation, unfriendly user interface, slow speed in uploading and downloading files, and delay in starting cloud applications. As a result, less than 50% of consumers consider personal clouds to be reliable, trustworthy and meeting their service level expectations. The fulfilment of consumer expectations encourages wider cloud uptake. If performance levels do not reach expectations because quality is compromised too much, consumers will reject the service or refuse adoption. Providers should thus pay more attention to the user experience.

Include minimum service levels in standard contracts. Although some cloud service providers undertake to make necessary backups, only one of the providers that we investigated warrant data integrity, or accept liability for data loss. Minimum service level standards would make it easier for consumers to compare different services. Further, in addition to providing their detailed terms and conditions, cloud providers might 'translate' their detailed terms and conditions to provide consumers with an 'abridged version' that provides less 'legal speak' but is more likely to be read and understood by average consumers.

Work to establish standards for interoperability. Portability is a key for competition in cloud services. Personal cloud services are not fully interoperable, which creates some difficulty (inconvenience) in moving data across different service platforms. The industry has to work on voluntary interoperability standards. The lack of interoperability can lead to consumer lock-in by making switching from one service to another impossible, costly or unattractive.

Recommendations for Regulatory and Consumer Agencies

Consider mandatory data breach notification in future law reforms. The *Privacy Act 1988* and its accompanying Australian Privacy Principles regulate the handling of personal data. Nevertheless, the Act currently does not specify the obligation of personal cloud service providers to inform consumers in case of a data breach. Future law reforms need to consider mandatory data breach notification.

Monitor to ensure that free personal cloud services have the same consumer protection standards as paid services. Personal cloud providers do not provide warranties as to the availability and performance of cloud services. This means consumers could be subject to data loss if a service provider discontinues (or disrupts) its services for various reasons. However, the ACL stipulates consumer guarantees that cannot be excluded by service contracts. There is potentially a variation between the service providers' terms and applicable Australian laws whereby contract terms may limit the liability of a guarantee. Further, personal cloud contracts favour service providers as they can change the performance of the cloud services, such as in size, speed and file delivery mechanisms, without consumers' consent. This is one area that needs to be examined more closely to ensure that personal cloud contracts are consistent with the ACL. The issue is further complicated by the fact that most consumers use personal cloud services provided by international companies and there may be practical challenges in enforcing the relevant Australian laws when the provider is based overseas**.**

Prioritise the enforcement of ACL on major international personal cloud providers. Government agencies such as the ACCC might further prioritise enforcement of the ACL by international personal cloud service providers. In the meantime, educate **consumers** so that they are well informed about cloud products and services as well as the practical challenges of enforcing the ACL on overseas personal cloud providers. Consumers use cloud services from both Australian and overseas providers. There is a need for clarity as to which Australian regulations apply and the extent of protection or regulation that they afford to personal cloud consumers that use overseas providers. Although the ACL will ordinarily apply, there may be practical challenges in enforcing that regulation, for example, if the provider is located overseas.

Implement a protocol for cloud computing to encourage information disclosure by cloud providers and support consumers of cloud services in being well informed. The ACS in consultation with the Australian government has initiated a discussion paper on an NCCP. At the time of the consultation, in 2013, there was a lack of support for an NCCP from major cloud vendors, industry bodies and telecommunications providers. These stakeholders considered that the protocol would replicate existing regulatory protections and complaints mechanisms that were already deemed effective. However, we believe that a national protocol can provide a consistent approach to cloud service providers to be upfront with consumers in response to data privacy and security issues and facilitate the integration of cloud services with extant Australian consumer protection and privacy laws.

Ensure that the personal information collected by personal cloud providers (particularly overseas personal cloud providers) meets the definition of personal information under the *Privacy Act 1988* and the method of data collection and its use comply with the Australian Privacy Principles.

Reassure consumers that are concerned about personal cloud–related digital surveillance that, unless a warrant is issued, existing regulations provide sufficient protection to the confidentiality of consumers' data during transmission and storage. Consumers need to be taught that it is easy to intercept data transmitted across unencrypted wi-fi networks.

Establish (or clarify) the mechanism for addressing personal cloud disputes. Unless a personal cloud service is provided by a carriage service provider, it is unlikely that the TIO (which focuses on the supply of landline, mobile and internet communications), can provide dispute resolution services

to personal cloud consumers. It is also important to look into whether the TCP provides adequate coverage to the privacy, billing, customer transfer and complaint-handling issues of personal cloud services.

Authors

Associate Professor Alemayehu Molla

Alemayehu Molla is an Associate Professor of Information Systems at RMIT's School of Business IT and Logistics. Before Joining RMIT, he was a Lecturer at The University of Manchester (UK) and the Addis Ababa University (Ethiopia). Alem's research interests include sustainable digital business, enterprise systems and development informatics. He has published more than 100 articles including in top-tier information systems (IS) journals, with 2400 Google Scholar citations and h-index 25.

Associate Professor Vanessa Cooper

Vanessa Cooper is an Associate Professor of Information Systems at RMIT University. Vanessa has published over 50 articles in Information Systems and Education outlets. Prior to entering academia Vanessa worked as a systems engineer within the finance and insurance industries in Australia and the United Kingdom and brings this expertise to her teaching and research activities.

Dr Ahmad Abareshi

Ahmad Abareshi is a Senior Lecturer at the School of Business IT and Logistics at RMIT University. He received his PhD degree in Information Systems from RMIT University. He is now Deputy Program Director Masters of Logistics and Supply Chain Management. Dr. Abareshi's research interests include green IT and green logistics. His research has appeared in a variety of academic journals including, among others, Information Technology & People, International Journal of Logistics Research and Applications, and Australasian Journal of Information Systems.

Dr Siddhi Pittayachawan

Siddhi Pittayachawan is a Senior Lecturer of Information Systems and Supply Chain Management in the School of Business IT and Logistics at RMIT University. He has xperiences in research and data analytical methods and is a versatile research methodologist. His reseaerch interest interests include trust, information system adoption, information security behaviour, sustainable business, supply chain management, and business education. His work has been cited over 300 times.

Glossary

Definitions of terms commonly used in this document are contained here.

ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ACS	Australian Computer Society
ANZCSO	Australian and New Zealand Standard Classification of Occupations
API	Application programming interface
CFA	Consumer Federation of America
DBCDE	Federal Government Department of Broadband, Communications and the Digital Economy
NCCP	National cloud computing protocol
NIST	National Institute for Standards and Technology
TCP	Telecommunications Consumer Protections
TIO	Telecommunications Industry Ombudsman

Figures and Tables

Figures

Figure 1 Types of personal cloud services ---- 13
Figure 2 Personal cloud awareness ---- 15
Figure 3 Frequently used personal cloud models ---- 16
Figure 4 Personal cloud payment ---- 20
Figure 5 Motivation for the personal cloud ---- 22
Figure 6 Personal cloud rhetorical experience, fear, attitude and trust ---- 23
Figure 7 Personal cloud self-efficacy ---- 24
Figure 8 Consumers' criteria for choosing a personal cloud ---- 27
Figure 9 Personal precautions for using a personal cloud ---- 28
Figure 10 Quality of experience ---- 29
Figure 11 Extra fees due to exceeding personal cloud limits ---- 30
Figure 12 Personal cloud consequences ---- 31
Figure 13 Users' personal cloud use continuance intention ---- 31
Figure 14 Non-users' intentions to adopt a personal cloud ---- 32
Figure 15 Distribution of most important and unimportant personal cloud issues ---- 34
Figure 16 Consumers' perception of the adequacy of current regulations ---- 36

Tables

Table 1 Summary of literature on the benefits of personal cloud 4
Table 2 Demographic profile of survey participants 10
Table 3 Personal cloud services used by consumers 17
Table 4 Comparison of a sample of personal cloud services (as of June 2015) 19
Table 5 Comparison of personal cloud terms of services 26
Table 6 Q-method interview items 33

APPENDICES

Appendix A: Profile of Interview and Focus Group Participants

Data	Unique ID	Gender	Description
Interview	Provider 1	Male	Founder and managing director of a company that offers a virtual PC desktop to consumers and a secure browser to protect consumer data while transacting on the internet
	Provider 2	Male	CEO and founder of a niche cloud service provider that enables consumers to use the internet with greater privacy, to collect their personal data and to own their 'digital footprint'
	Provider 3	Female	Managing director of a company that provides a personal cloud to consumers throughout Australasia and that focuses on 'personal sovereignty' (such as privacy) at the centre of each transaction
	Consumer Group 1	Male	Technology team leader of an organisation that identifies misleading or unhelpful practices and that tests products and services in a range of markets including technology to ensure that consumers get the most out of their purchasing decisions
	Consumer Group 2	Male	Project manager of digital and online technology in a not-for-profit organisation working to improve access to media for people with a disability
	Agency 1	Male	Senior manager of a statutory authority entrusted with ensuring that Australia's media and communications legislation, regulation, standards and codes of practice operate effectively
Focus Group	Consumer1	Male	Working full-time as a hairdresser; male
	Consumer 2	Male	Has postgraduate education and currently working in marketing research
	Consumer 3	Male	A screenwriter, author, actor and musician
	Consumer 4	Male	A librarian of 28 years' experience working in public and university-based libraries
	Consumer 5	Female	Works in a university as an administrator of student mobility programs; has over 16 years' experience in a range of administrative roles
	Consumer 6	Female	Is a non-IT professional working in administration but is exposed to technology (e.g. database and internet technology) in her professional and private life
	Consumer7	Female	Holds an administrative role that requires the use of technology; has 14 years of experience
	Consumer 8	Female	Has worked in an administrative role in a university for the past five years
	Consumer 9	Female	Holds a position in finance; has been using technology and the internet for many years
	Consumer10	Female	Female; working in an administrative role within a university for a decade; has used a lot of technology in her various roles but has not had much experience with a personal cloud apart from her iPhone
	Consumer 11	Female	A recent graduate undertaking a professional year and soon to be embarking on an internship as a business analyst
	Consumer 12	Male	An IT professional with 14 years' experience in the IT industry; his roles have covered test management, IT architecture, business

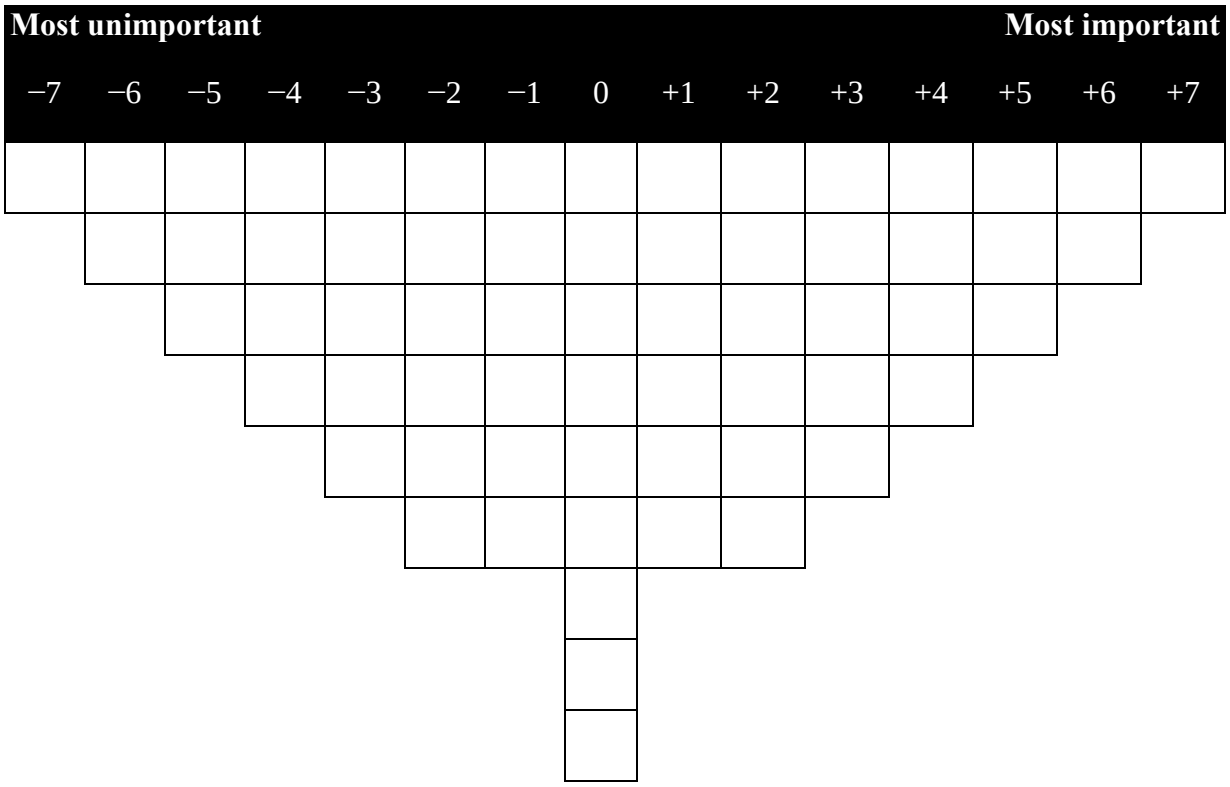
			analysis and business intelligence within the context of data warehouses
	Consumer 13	Male	An enterprise architect within the utilities sector; has over 15 years' experience in the IT industry
	Consumer 14	Female	A business IT graduate working as a data analyst on a customer relationship management system
	Consumer 15	Male	Works in product management sphere focusing on the digital marketing space
	Consumer 16	Male	An IT consultant with three years' experience, primarily in business analysis roles
	Consumer 17	Male	An academic with over 10 years' experience researching and teaching in the IT discipline
	Consumer 18	Male	Works as a business analyst in the financial services industry with a particular interest in technology
	Consumer 19	Male	An enterprise architect with over 22 years' experience who is currently working for a multinational IT services company in the financial services industry
	Consumer 20	Female	An IT professional with three years' post-university experience currently working as a team leader
	Consumer 21	Male	Undertaking a PhD in the School of Management at RMIT University; has 10 years' industry experience in banking and manufacturing
	Consumer 22	Female	Completing a Master of Project Management after working as an architect for three years
	Consumer 23	Female	Undertaking a PhD in operations management having completed a master's degree in the same field; has an engineering background and has worked as a researcher in finance for 12 months
	Consumer 24	Male	Completing a PhD in project and innovation of small–medium enterprises in Indonesia; has previously worked as a lecturer and is currently working as a research assistant; has prior experience working for a multinational corporation in Indonesia
	Consumer 25	Male	Doing a PhD on small industry; has a background in small business and teaching
	Consumer 26	Female	Currently doing a Bachelor of Fine Arts after working for 14 years in a bank
	Consumer 27	Female	Doing a PhD in the School of Business IT and Logistics; has five years' experience working in industry and 10 years in education
	Consumer 28	Female	Currently completing a PhD on environmental regulation and climate change and the financial market; previously completed a Bachelor of Statistics and worked as a statistician for six years
	Consumer 29	Male	Doing a PhD on the topic of climate change in multinational corporations; has 10 years' work experience in the government, non-government and educational sectors

Appendix B: Detailed Profile of Q-Interviewees

Participant	Age	Gender	Use	Services	Exp	Paid	Devices	Platforms	Size
P1	34	M	B	Gmail (17 yr), Google Drive, Dropbox ($100/yr) OneDrive, iCloud, Facebook, LinkedIn, Twitter, YouTube	17 yr	Y			
P2	24	M		Google, Box	<10 yr	N			
P3	36	M	B	Dropbox, Google Drive, iCloud	4–5 yr	N			
P4	52	M	B	Dropbox (4–5 yr), Linux DIY (23–24 yr), OneDrive, Facebook, Picasa, Prezi	23–24 yr	N	Tablet, notebook PC (H), PC (W) mobile phone	Android Windows 7/8	
P5	38	M	B	iCloud, Google Drive	3–4 yr	N			
P6	31	M	B	Dropbox, OneDrive, Google Drive, Facebook	8 yr	N	iPad PC	iOS	
P7	69	M	B	Dropbox, iCloud, Google Drive, OneDrive, Amazon	6 yr	N	Tablet	iOS	
P8	39	M	B	Dropbox (5–6 yr), Amazon (1.5 yr), iCloud	5–6 yr	N			
P9	66	M	W	Dropbox, Google Drive	1 yr	N	iPhone 5, Sony Xperia		
P10	50	M	W	Dropbox ($100/yr), Google Drive, FTP (30 yr)	30 yr	Y	Tablet, notebook, PC	Android Windows	>10 GB
P11	29	M	B	Hotmail	10 yr	N			
P12	62	M	B	Dropbox (4–5 yr, $100/yr) Google Docs, Diigo, Delicious, Picasa	4–5 yr	Y	Phone, tablet, PC (H)		50 GB
P13	38	M	B	Yahoo Mail, Gmail, Google Drive, Facebook Skype, Orkut		N			
P14	33	M	B	OneDrive, Gmail Google Drive, iCloud. Facebook	8–10 yr	N	iPhone	iOS	40 GB
P15	59	M	B	Dropbox, Facebook, LinkedIn		N			5–10 GB
P16	41	F	W	Amazon	6–8 yr	N			2–3 GB
P17	30	F	P	Dropbox, iCloud	4 yr	N	iPhone, MacBook, iPad, PC (W)	iOS Android Mac OS	DK
P18	34	F	B	iCloud, Friendster, Facebook (8 yr), YouTube Vimeo, Dropbox (2 yr), Google Drive, Yahoo Mail (17 yr), Hotmail, Prezi, Yammer	17 yr	N			DK
P19	54	F	W	Google Drive		N	Lenovo, Android, Samsung tablet	Android	DK
P20	47	M	B	WhatsApp, LINE,	10 yr	Y	iMac	Mac OS	

				Snapchat, Instagram (6 yr) Facebook (6 yr), Dropbox (6 yr, $100/yr), Google Drive, OneDrive, Gmail (10 yr), email (DIY) ownCloud (DIY), WeChat (2 yr), Prezi, Balsamiq, OneNote (2 yr), Hotmail, EndNote Web, LinkedIn					
P21	50	F	B	iCloud, Dropbox (1 yr), Facebook, LinkedIn, ResearchGate, Google (3 yr), Hotmail (>10 yr), Yahoo Mail, Skype		N			DK
P22	45	M	W	Dropbox (2–3 yr), Google Drive	2–3 yr	N	PC (W), laptop	Windows	
P23	47	M	B	Google, Dropbox, iCloud, LinkedIn, Skype StoryBoard ($100/yr)	5–6 yr	Y			1 GB
P24	40	M	B	Dropbox, Google, Photobucket, Facebook (5 yr), Prezi	3–4 yr	N	iPad, Samsung mobile		DK
P25	55	M	B	Gmail (enterprise) Gmail (signup only)		N			
P26	58	F	B	iCloud (3 yr)	3 yr	Y			DK

Appendix C: Q-interview Sorting Scale



Appendix D: Sample of a Completed Q-interview Sheet

Most Unimportant													Most Important	
−7	−6	−5	−4	−3	−2	−1	0	+1	+2	+3	+4	+5	+6	+7
57	40	14	48	7	43	55	44	53	35	56	25	58	1	3
	41	13	37	10	19	26	51	42	54	31	28	33	2	
		39	20	15	29	22	60	63	17	23	32	4		
			61	16	9	36	38	45	50	24	62			
				5	6	8	18	59	47	34				
					11	46	27	21	12					
							52							
							49							
							30							

Appendix E: Six Distinct Groups of Personal Cloud Consumers

Participant	Group 1	Group 2	Group 3	Group 4	Group5	Group6
P16	**0.8628**	–0.2041	–0.0770	0.0456	–0.0093	0.1130
P8	**0.8150**	–0.0063	0.1550	0.1057	–0.1933	–0.0800
P4	**0.8029**	0.2178	–0.5390	–0.1465	0.0804	0.0630
P1	**0.7550**	0.1079	–0.0610	0.2293	–0.0320	–0.1420
P9	**0.7549**	–0.4896	0.0990	–0.0089	0.2255	–0.1510
P25	**0.7301**	–0.3495	0.1250	0.1134	0.0938	0.2290
P7	**0.6562**	0.2845	–0.0550	–0.2750	–0.2314	0.0720
P2	**0.6424**	0.1109	0.2960	0.0876	–0.3134	–0.0170
P12	**0.5842**	0.2664	0.0830	–0.1637	0.2947	–0.2420
P22	**0.5753**	0.0633	0.0330	0.1425	0.2383	–0.1120
P6	**0.5128**	0.2370	0.0790	–0.0028	0.1823	0.1460
P23	**0.4636**	0.2859	0.2220	0.0976	0.0404	0.1220
P20	0.1090	**0.8038**	–0.1110	0.2211	0.0113	0.1450
P18	0.0719	**0.7945**	–0.0880	0.1566	0.1756	–0.0440
P10	0.0546	**0.7556**	0.0360	0.2396	0.0104	0.0580
P5	0.1267	**0.6596**	0.2150	–0.1177	0.0361	0.0390
P15	–0.0078	–0.1816	**0.8120**	0.1566	0.0554	0.1410
P19	0.2381	0.0647	**0.6830**	–0.1306	0.0438	–0.1260
P21	–0.2961	0.1819	**0.6770**	0.1862	0.1720	0.0560
P3	0.3453	–0.0068	**0.5790**	–0.0661	0.0074	0.1330
P17	0.3195	0.1306	–0.0740	**0.7834**	–0.1885	–0.0990
P11	–0.1713	0.3461	0.1980	**0.6675**	–0.0394	–0.1450
P24	0.1589	0.1248	0.0640	–0.1180	**0.7370**	0.0560
P13	0.1022	0.1098	0.1850	–0.1220	**0.6523**	–0.0160
P26	–0.0517	0.1115	–0.1230	0.0535	0.0927	**0.8320**
P14	0.0521	0.1091	0.3240	–0.3381	–0.0488	**0.6410**
n	***12***	***4***	***4***	***2***	***2***	***2***
Eigenvalue	***6.2***	***3.3***	***2.7***	***1.7***	***1.5***	***1.5***
Expl var (%)	***23.8***	***12.7***	***10.4***	***6.4***	***5.8***	***5.6***
Reliability	***0.98***	***0.94***	***0.94***	***0.89***	***0.89***	***0.89***

Appendix F: Correlation among the Six Groups

	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
Group 1	1					
Group 2	0.39	1				
Group 3	0.48	0.46	1			
Group 4	0.37	0.34	0.39	1		
Group 5	0.48	0.41	0.51	0.21	1	
Group 6	0.24	0.38	0.16	0.01	0.22	1

Appendix G: Crib Sheet

The table summarises the statement factor scores that are used to create ‘a crib sheet’ for each group and interpret the views and characteristics of each group.

Statement	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
1	6	5	7	7	6	2
2	4	0	5	2	3	0
3	7	2	6	4	5	–2
4	5	4	5	4	1	1
5	–4	–7	–2	–4	4	–6
6	1	2	–1	1	–2	4
7	0	4	–6	–2	–2	–2
8	2	3	2	3	2	–1
9	–1	6	1	–3	7	7
10	–2	1	–3	–5	1	2
11	2	7	2	0	0	2
12	–1	6	2	1	–3	0
13	–6	0	4	–3	–6	1
14	–5	2	3	2	4	1
15	–4	0	5	0	2	3
16	–4	1	3	0	–4	–1
17	1	3	2	0	0	6
18	–1	0	–3	2	–2	–2
19	–2	–3	0	–5	0	–3
20	–1	1	0	0	–2	–4
21	0	0	0	–2	3	–4
22	0	2	–2	–6	1	5
23	4	5	0	–1	0	4
24	3	3	3	5	0	3
25	5	2	0	–3	4	3
26	0	–3	–4	–1	–4	2
27	0	–1	–2	–2	0	2
28	3	1	–3	–2	1	5
29	3	4	0	1	1	0
30	–1	–1	–1	–4	–5	3
31	–2	–1	1	0	2	1
32	4	3	4	6	–2	1
33	5	2	2	2	6	4
34	2	–2	1	–5	3	–4
35	2	1	3	5	3	0
36	0	–1	2	–4	0	1
37	–4	–6	–2	–6	–6	1
38	–3	–4	–3	–3	–2	3
39	–5	4	–1	0	–1	–3
40	–7	0	0	2	4	–2
41	–6	0	–4	0	–1	–1
42	2	0	4	2	5	0
43	–3	–3	–5	–4	–5	–5
44	–2	–2	0	0	–1	–6
45	0	–2	–1	6	–4	0
46	–2	–6	–5	–7	–3	–1
47	3	–4	1	–1	–1	–4
48	–3	0	–1	–3	–1	–2
49	1	5	–1	5	3	4

50	–3	–5	–2	–1	–4	6
51	2	1	3	–2	1	–3
52	–1	–2	–2	4	–1	0
53	0	–4	–4	2	2	0
54	0	–1	–5	–1	–1	3
55	1	–5	–3	–2	–3	0
56	3	–4	4	3	2	0
57	–5	–2	–7	–1	–5	–7
58	6	3	6	1	5	–1
59	–2	–2	–4	4	–3	–3
60	1	–1	1	3	–3	–3
61	–3	–5	0	1	–7	–5
62	4	–3	1	–2	2	–2
63	1	–3	–6	3	0	–5

References

ACMA—*see* Australian Communications and Media Authority.

ACS—*see* Australian Computer Society.

AGIMO—*see* Australian Government Information Management Office.

Andersen, A & Karlsen, R 2011, 'Personal information and the personal cloud', *NIK (Norsk informatikkonferanse) 2011 Conference, Norway, Oslo, pp. 1-4*.

Ardissono, L, Goy, A, Petrone, G & Segnan, M 2009, 'From service clouds to user-centric personal clouds', *IEEE International Conference on Cloud Computing*, IEEE, Bangalore, pp. 1–8.

ATSE—*see* Australian Academy of Technological Sciences and Engineering.

Australian Academy of Technological Sciences and Engineering 2010, *Cloud computing: opportunities and challenges for Australia*, Melbourne, Australia.

Australian Communications and Media Authority 2013, *The cloud—services, computing and digital data: emerging issues in media and communications*, Occasional Paper 3, <viewed 5 September. 2014,http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/The%20cloud%20services%20computing%20and%20digital%20data%20Emerging%20issues%20in%20media%20and%20communications.pdf>.

Australian Communications and Media Authority 2014, *Report 2—Cloud computing in Australia*, viewed 25 April2015, <http://www.acma.gov.au/~/media/Research%20and%20Reporting/Report/pdf/Cloud%20Computing%20report_final%20pdf.pdf>.

Australian Computer Society 2013a, *Cloud computing consumer protocol*, ACS Cloud Discussion Paper, viewed 5 April 2015, <http://www.acs.org.au/__data/assets/file/0018/21672/ACS-Cloud-Discussion-Paper.pdf>.

Australian Computer Society 2013b, *ACS cloud protocol consultation: report on the outcomes of the ACS public consultation of Cloud Protocol*, viewed 29 July 2014, <https://www.acs.org.au/__data/assets/pdf_file/0017/27800/ACS-Cloud-Protocol-Consultation-Report.pdf>.

Australian Government 2010, *The Australian consumer law: an introduction*, viewed 6 April 2015, <http://www.consumerlaw.gov.au/content/the_acl/downloads/ACL_an_introduction_November_2010.pdf>.

Australian Government Information Management Office 2014, *Community cloud governance—An Australian Government perspective: better practice guide*, Australian Department of Finance and Deregulation, viewed, 7 April 2015, <http://www.finance.gov.au/policy-guides-procurement/cloud/>.

BEUC 2013, *BEUC's contribution on cloud computing for the public hearing in the ITRE Committee, European Parliament, 29 May 2013,* <viewed 27 July 2014, http://www.europarl.europa.eu/document/activities/cont/201306/20130604ATT67273/20130604ATT67273EN.pdf>.

Bhattacharyya, S, Sen, M & Agarwal, S 2012, 'Battling the fear of heights: pros and cons of the personal cloud', *International Conference on Communication Systems and Network Technologies*, IEEE, Rajkot, pp. 726–730.

CAL—*see* Communications Alliance Limited.

CFA—*see* Consumer Federation of America.

Communications Alliance Limited 2012, *Telecommunications Consumer Protections Code* (C628:2102), viewed 6 April 2015, <http://www.commsalliance.com.au/__data/assets/pdf_file/0017/33128/TCP-C628_2012_May2012-Corrected-July12.pdf>.

Consumer Federation of America 2010, *Consumer protection in cloud computing services: recommendations for best practices from a CFA retreat on cloud computing*, viewed 6 July 2014, <http://www.consumerfed.org/pdfs/Cloud-report-2010.pdf>.

DBCDE—*see* Department of Broadband, Communications and the Digital Economy.

Department of Broadband, Communications and the Digital Economy 2013, *The National Cloud Computing Strategy*, viewed 29 July 2014, <http://www.communications.gov.au/data/assets/pdf_file/0008/163844/National_Cloud_Computing_Strategy.PDF>.

Department of Communications 2014, *Cloud computing regulatory stock take*, <viewed 1 April 2015, https://www.communications.gov.au/publications/cloud-computing-regulatory-stock-take-report%C2%A0 >.

DOC—*see* Department of Communications.

Drago, I, Bocchi, E, Mellia, M, Slatman, H & Pras, A 2013, 'Benchmarking personal cloud storage', *Proceedings of the 2013 Internet Measurement Conference*, ACM, Barcelona, Spain, pp. 205–212.

Drago, I, Mellia, M, Munafo, M, Sperotto, A, Sadre, R & Pras, A 2012, 'Inside Dropbox: understanding personal cloud storage services', *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, ACM, Boston, Massachusetts, pp. 481–494.

Ernst, J 2012, 'What is a personal cloud?', viewed 10 November 2014 <http://iiw.idcommons.net/What_is_a_Personal_Cloud%3F>.

Fahl, S, Harbach, M, Muders, T & Smith, M 2012, *Confidentiality as a service—usable security for the cloud*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 25–27 June, Liverpool.pp 153-162.

Gartner 2012, *Competitive landscape: consumer personal cloud*, viewed 8 July 2015, <https://www.gartner.com/doc/1967316/competitive-landscape-consumer-personal-cloud>.

Gewirtz, D 2013, *Security implications of public vs. private clouds*, viewed 8 July 2015, <http://www.zdnet.com/article/security-implications-of-public-vs-private-clouds/>.

Gillett, FE, Mines, C, Schadler, T, Yamnitsky, M, Shey, H, Martland, A & Iqbals, R 2011, *The personal cloud: transforming personal computing, mobile, and web markets*, BT Futures Report, Forrester Research, Cambridge, MA.

Gnesi, S, Matteucci, I, Moiso, C, Mori, P, Petrocchi, M & Vescovi, M 2014, 'My data, your data, our data: managing privacy preferences in multiple subjects personal data', B. Preneel & D. Ikonomou (eds) *Privacy technologies and policy*, Springer,Switzerland, pp. 154–171.

Gracia-Tinedo, R, Artigas, MS & Lopez, PG 2013a, 'Cloud-as-a-gift: effectively exploiting personal cloud free accounts via REST APIs', *2013 IEEE Sixth International Conference on Cloud Computing (CLOUD)*, IEEE, Santa Clara, CA, pp. 621–628.

Gracia-Tinedo, R, Artigas, MS, Moreno-Martinez, A, Cotes, C & Lopez, PG. 2013b, 'Actively measuring personal cloud storage', *IEEE Sixth International Conference on Cloud Computing (CLOUD*), IEEE, Santa Clara, CA, pp. 301–308.

Hobfeld, T, Schatz, R, Varela, M & Timmerer, C 2012, 'Challenges of QoE management for cloud applications', *IEEE Communications Magazine*, vol. 50, no. 4, pp. 28–36.

Hon, WK, Millard, C & Walden, I 2012, 'Who is responsible for "personal data" in cloud computing?—The cloud of unknowing', Part 2, *International Data Privacy Law*, vol. 2, no. 1, pp. 3–18.

Hustinx, P 2012, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"', European Data Protection Supervisor, Brussels.

Jun, CJ, Lee, JH & Young, D 2013, 'Research about factor affecting the continuous use of cloud storage service*', 12th International Decision Sciences Institute Conference,* July 9–13, Bali, Indonesia.

Kuyoro, S, Ibikunle, F & Awodele, O 2011, 'Cloud computing security issues and challenges', *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247–255.

Ky, S 2014, 'Managing consumerization of personal cloud storage: a New Zealand perspective' (), *School of Information Management*, School of Information Management, Victoria University of Wellington, Wellington.

Lewallen, MC 2013, *Cloud computing: a lawyer's ethical duty to act with reasonable care when storing client confidences in the cloud*, viewed 21 September 2014. http://heinonline.org/HOL/Print?collection=journals&handle=hein.journals/clevslr60&id=1149&print=section&section=39&ext=.pdf.

Li, A, Yang, X, Kandula, S & Zhang, M 2010, 'CloudCmp: comparing public cloud providers', *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, ACM, Melbourne, Australia, pp. 1–14.

Marnau, N, Jensen, M, Schlehahn, E & Ferrer, RM 2012, *Cloud computing: solutions and enablers,* <viewed 15 August 2014, http://www.tclouds-project.eu/downloads/deliverables/TC-D1.2.3-Cloud-Computing-Solutions-and-Enablers_M24.pdf>.

Marshall, C & Tang, JC 2012, 'That syncing feeling: early user experiences with the cloud', *Proceedings of the Designing Interactive Systems Conference,* ACM, June 11–15, 2012 • Newcastle, UK**,** viewed 15 August 2014http://dl.acm.org/citation.cfm?id=2318038.

Martic, D 2013, *'*Online dispute resolution for cloud computing services*', Proceedings of the First JURIX Doctoral Consortium and Poster Sessions in conjunction with the 26th International Conference on Legal Knowledge and Information System*, Bologna, Italy.

Mell, P & Grance, T 2011, *The NIST definition of cloud computing*, US Department of Commerce, <viewed 15 February 2014, http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>.

Mohammed, D 2011, 'Security in cloud computing: an analysis of key drivers and constraints', *Information Security Journal: A Global Perspective*, vol. 20, no. 3, pp. 123–127.

Moqbel, M, Bartelt, V & Al-Suqri, M 2014, 'A study of personal cloud computing: compatibility, social influence, and moderating role of perceived familiarity', *Twentieth Americas Conference on Information Systems*, Savannah, pp. 1–10.

Na, SH, Park, JY & Huh, EN 2010, 'Personal cloud computing security framework', *2010 IEEE Asia-Pacific Services Computing Conference (APSCC)*, Hangzhou, pp. 671–675.

Pyramid Research 2014, 'The personal cloud: a strategic imperative for operators—Competitive market trends, forecasts and operator business models', viewed 15 August 2014, <www.ReportLinker.com>.

Qiong, S, Liu, M & Pang, S 2013, 'Cloud computing application of personal information's security in network sales-channels', *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 11, no. 12, pp. 7331–7338.

Ried, S, Kisker, H & Matzke, P 2010, 'The evolution of cloud computing markets', *Forrester Research*.

Rivera, J 2010, 'Cloud computing for personal use', *The Epoch Times*, viewed 8 July 2015, <http://www.theepochtimes.com/n2/technology/cloud-computing-for-personal-use-29794.html>.

Steger, H & Funambol 2012, *'*The cloud storage services battle: what every mobile provider should know*', Wireless Week*, 17 May, viewed 14 July 2014, <http://www.wirelessweek.com/articles/2012/05/cloud-storage-services-battle-what-every-mobile-provider-should-know>.

Teneyuca, D 2011, 'Internet cloud security: the illusion of inclusion', *Information Security Technical Report*, vol. 16, no. 3, pp. 102–107.

Thomas, DM & Watson, RT 2002, 'Q-sorting and MIS research: a primer', *Communications of the Association for Information Systems*, vol. 8, no. 1, pp. 140-157..

Vandenbroucke, K, De Moor, K & De Marez, L 2013, 'Use- and QoE-related aspects of personal cloud applications: an exploratory survey', paper presented at *The 2013 Fifth International Workshop on Quality of Multimedia Experience (QoMEX),* Klagenfurt, 3–5 July 2013.

Wattal, S, Racherla, P & Mandviwalla, M 2010, 'Network externalities and technology use: a quantitative analysis of intraorganizational blogs', *Journal of Management Information Systems*, vol. 27, no. 1, 2010, pp. 145–174.

Legislation

Australian Competition and Consumer Act 2010 (Cwlth).

Copyright Amendment (Online Infringement) Bill 2015

Privacy Act 1988 (Cwlth).

Telecommunications Act 1997 (Cwlth).

Telecommunications (Interception and Access Act) 1979 (Cwlth).

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cwlth).