COMPUTER LAW & SECURITY REVIEW XXX (2015) 1–28

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

CloudConsumer: contracts, codes & the law☆

*Kate Mathews Hunt**

School of Law, Bond University, Gold Coast, Australia

Keywords:
Cloud computing
Consumer law
Misleading deceptive conduct
Consumer guarantees
Unfair contract terms
False representations
Australia

ABSTRACT

This consumer cloud is in serious flux. Consumers have, perhaps inadvertently, flocked to the cloud via unpaid social media, storage and email offerings, whilst resisting paid cloud take-up for reasons (inter alia) of cost, resources, technical ignorance and security. Yet consumers are taking a storage, privacy and data risk in the 'free' cloud, and there is a growing consciousness of this fact. At present however, (non) buyer beware or "you get what you pay for" seems to be the prevailing industry – and consumer – expectation. The result is that individual and small business consumers are caught in a gap between paid and unpaid offerings; one which this paper explores through a consumer law view of cloud computing. An examination of Australian consumer law reveals that cloud provision is, like most other consumer 'goods' or 'services', covered under Australian law, and in particular, the laws governing false and misleading conduct, unconscionability, statutory guarantees and unfair contract terms. The paper considers these laws and industry regulatory solutions such as the New Zealand *CloudCode*, together with considering various cases brought to date, future developments and proposing future responses. The underlying prediction is that the emerging issue of consumer cloud integrity may present an impediment to wider individual/small business uptake, and that consumer law may emerge as an effective redress for this perceived market failure, and offer potentials to reshape the industry from a consumer perspective. The author concludes with the view that the cloud industry has significant risk assumption, contractual simplification and educative communication work yet to do to better encourage consumer paid cloud uptake and more universal adoption.

☆ READERS NOTE: This paper is a 'lawyer's look' at cloud computing from the consumer perspective; it does not purport to offer a technical, industry-based or practical analysis of either the cloud or its inherent security and privacy issues. These technical matters are far better dealt with by experts in these fields and the author does not pretend to have any computing expertise beyond that of an average Australian consumer. As such technical errors are intended to be avoided, but may be inevitable.

* Faculty of Law, Law Building, Bond University, University Drive, Robina, Queensland 4229, Australia.
E-mail address: kmathews@bond.edu.au.

http://dx.doi.org/10.1016/j.clsr.2015.05.006
0267-3649/

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

...The Cloud is about trust... [1]

...trusting data to the cloud borders on an act of faith... [2]

...it's going to be horrendous... there's going to be a lot of horrible problems in the next five years... [3]

1. Introduction

The cloud[4] is the perfect high tech storm. In todays "quicksilver technological environment",[5] the vision is of blue sky opportunity and limitless promise. Digital data is the new 'currency'[6] of the digital economy,[7] cloud computing is the bank vault and cloud providers hold the keys to twenty-first century business productivity and success.[8] Cloud adoption is hailed as an "evolving paradigm",[9] "... a transformative journey that will catalyse change across the organization",[10] but without action, can remain "vague and aspirational".[11] But for other commentators, the cloud is "fraught with controversy and nuance,"[12] and "... difficult to know where the boundaries are."[13] Clearly, the cloud attracts a "thesaurus of hyperbole"[14] – on the one hand, it is "revolutionary, irresistible,"[15] and on the other, critics accuse the industry of marketing a "myth of total virtualization"[16] using a "... somewhat over-hyped ... sales buzzword".[17] Gartner have recently predicted that the term is becoming so ill-defined that it may soon "disappear"[18] altogether.

This paper puts the view that the consumer cloud is in serious flux. Consumer ignorance as to what constitutes a cloud service is demonstrable,[19] whilst recent highly-publicised privacy and security breaches with significant consumer consequences and service provider reputational damage,[20] have ensured that the 'cloud' remains potentially suspect. Consumers have, perhaps inadvertently, flocked to the cloud via unpaid social

[1] Institute of IT Professionals, 'New Zealand *CloudCode*, Cloud Computing Code of Practice' (v 2.0) (2013 accessed 11 June 2014) [clause 1] <www.thecloudcode.org/>.

[2] GreenSQL CEO Amir Sadeh quoted in GreenSQL, 'GreenSQL October Survey – 81% of IT Professionals Have Security Concerns When Moving Data to the Cloud' (November 19, 2012 accessed 17 June 2014) <http://www.greensql.com/pressroom/news/2013/05/30/greensql-october-survey>.

[3] Steve Wozniak, Apple co-founder cited in August 2012 as reported by http://www.france24.com/en/20120805-apple-co-founder-wozniak-sees-trouble-cloud and cited in Infoworld, 'Apple iCloud breach proves Wozniak's point about cloud risks' *InfoWorld Tech Watch* (6 Aug 2012 accessed 2 June 2014) <http://www.infoworld.com/t/cloud-security/apple-icloud-breach-proves-wozniaks-point-about-cloud-risks-199450?source=footer>.

[4] The term 'cloud' means: "On-demand scalable resources such as networks, servers and applications which are provided as service, are accessible by the end-user and can be rapidly provisioned and released with minimal effort or service provider interaction": above n 1. Note that this simplified version of the NIST definition expressly incorporates the latter in clause 2.

[5] Urs Gasser, 'Cloud Innovation and the Law: Issues, Approaches, and Interplay' Harvard University - Berkman Center for Internet & Society; University of St. Gallen (March 17, 2014 accessed 20 June 2014) [2] Berkman Center Research Publication No. 2014-7 http://cyber.law.harvard.edu/research/cloudcomputing.

[6] Meglena Kuneva, European Consumer Commissioner (March 2009) cited in ACMA, 'The cloud: services, computing and digital data—Emerging issues in media and communications, Occasional paper 3' (June 2013 accessed 11 July 2014) [1] <http://www.acma.gov.au/~/media/Regulatory%20Frameworks/pdf/The%20cloud%20services%20computing%20and%20digital%20data%20Emerging%20issues%20in%20media%20and%20communications.pdf.

[7] The 'digital economy' refers to the global network of social and economic activities enabled by platforms such as the internet, mobile and sensor networks: Commonwealth of Australia, 'Department of Broadband, Communications and the Digital Economy: Annual Report' (2013 accessed 6 June 2014) [18] <http://www.communications.gov.au/__data/assets/pdf_file/0020/182018/1595_DBCDE_Annual_Report_WEB_FA_V3.pdf.

[8] The Cloud Infographic, 'The Impact of Cloud and Mobile in your Life' (6 Mar 2014 accessed 16 June 2014) <http://www.thecloudinfographic.com/2014/03/06/the-impact-of-cloud-and-mobile-in-your-life.html>.

[9] Peter Mell & Timothy Grance, 'The NIST Definition of Cloud Computing', US National Institute for Standards & Technology (NIST), Special publication 800-145, (September 2011 accessed 6 July 2014) [1 para 1.2] <http://csrc.nist.goiv.publications/nistubs/800-145/SP800-145.pdf.

[10] Egidio Zarella, KPMG China cited in KPMG International, 'The Cloud takes Shape' (2013 accessed 7 July 2014) [9] <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/the-cloud-takes-shapev3.pdf>.

[11] Ibid: 9.

[12] Mell: above n 9.

[13] Phillip C. Roberts, 'Submission to the Australian Computer Society: Cloud Computing Consumer Protocol' (19 Aug 2013 accessed 17 June 2014) <http://www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol/2013-australian-cloud-protocol-submissions>.

[14] Orton-Jones, Charles, 'A Cloudy Start For Business Promises A Bright Future' *Raconteur* (11th July 2013 accessed 18 June 2014) <http://raconteur.net/technology/a-cloudy-start-for-business-promises-a-bright-future>.

[15] Ibid.

[16] Arcserve, 'Meeting Business data protection Needs in a Mixed Physical/Virtual Environment' (2013 accessed 1 July 2014) http://www.findwhitepapers.com/force-download.php?id=37811.

[17] King, Leo 'Heading into Cloud with Eyes Open' *Raconteur* (11th July 2013 accessed 18 June 2014) <http://raconteur.net/technology/heading-into-the-cloud-with-eyes-wide-open>.

[18] "Cloud fatigue will be one of the main drivers toward decline in the use of the term "cloud" in IT environments. Cloud will continue to be used as a generic business term, not unlike e-business, and will eventually fade in that arena as well. Business-led initiatives will increasingly be aligned with the broader Nexus of Forces (cloud, mobile, social and information). Cloud computing will continue to be used as a term as long as it is meaningful (e.g., can be used to differentiate from non-cloud offerings). This is becoming harder for many reasons, including ongoing confusion.": Gartner, 'Predicts 2013: Cloud Computing Becomes an Integral Part of IT' (04 December 2012 accessed 18 June 2014) <https://www.gartner.com/doc/2263916?ref=SiteSearch&sthkw=cloud%20computing&fnl=search&srcId=1-3478922254>.

[19] See for example, Curator, Stern 'ACMA assesses consumer & SME cloud usage' *WhaTech* (May 2014 accessed 11 July 2014) <http://www.whatech.com/cloud-computing/20608-bit421-acma-assesses-consumer-sme-cloud-usage>.

[20] See the discussion at part 3.2 below. See also Taylor Amerding, 'The 15 Worst Data Security breaches of the 21st Century' CSO (15 Feb 2012 accessed 29 May 2014) www.csoonline.com/article/700263.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

media, storage and email offerings,[21] whilst resisting paid cloud take-up for reasons (inter alia) of cost, resources, technical ignorance and security.[22] The policy problem is real, given KPMG suggest greater consumer/SME[23] cloud take-up could yield cost savings in 2014 which could add $2–3 billion to GDP.[24] The previous Australian government has acknowledged this serious issue in pursuing policy settings designed to promote commercial internet interaction, encouraging a consumer-based cloud code solution to the industry[25] and by prioritising government departmental cloud adoption[26] – but these efforts have met with varied success. While Australia may be "cloud ready",[27] it seems that most prudent legal[28] and expert technical advice[29] on cloud usage recommends that business retain critical database servers within a 'private' environment only. In contrast, the consumer cloud is largely a public space of unprecedented convenience, with the hidden trade-off of an inherently insecure and seemingly, legally unaccountable environment.[30] Consumers are taking a storage, privacy and data risk in the 'free' cloud, and there is a growing consciousness of this fact,[31] but in the end, (non) buyer beware or "you get what you pay for"[32] seems to be the prevailing industry – and consumer – expectation.[33] The result is that individual and small business consumers[34] are caught in a gap; commercial cloud solutions may be too expensive, technically difficult or daunting to adopt, whilst consumer cloud solutions offer potentially catastrophic security issues or inappropriate environments for critical personal information and important business data.

This paper explores this gap through a consumer law view of cloud computing; that is, it aims to consider the cloud from the perspective of its risks and benefits to consumers under the *Australian Consumer Law* and to identify potential consumer issues which exist in a cloud computing context. That context is one in which traditional legal concepts are at times, an awkward

[21] Examples include facebook, dropbox and gmail.

[22] Jim Minifie, 'The silver lining: cloud computing and small and medium enterprises A Grattan paper' *Grattan Institute* (June 2014 accessed 17 June 2014) [1] <http://grattan.edu.au/publications/reports/post/the-silver-lining-cloud-computing-and-small-and-medium-enterprises/>.

[23] SMEs are defined to mean small and medium enterprises, which employ less than 200 employees. 'Small' business employ less than 20 staff and medium, from 20 to 199: Australian Communications Media Authority (ACMA) 'Report 1- Australian SME's in the digital economy' Communications Report 2012-13 series (Jan 2014) [1] <http://www.acma.gov.au/~/media/Communications%20.

[24] KPMG, 'Modelling the economic impact of Cloud Computing' *Report to Australian Information Industry Association* (2012 accessed 14 July 2014) <https://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf> Based upon 2012 GDP levels, and positing cloud adoption across 75% of IT spending and achieving opex (25%) and capex (50%) savings, KPMG estimate an increase in long run GDP of $3.32 billion per annum after ten years.

[25] See the discussion in Part 4 below.

[26] In 2013, the previous Australian Government devised a national cloud computing strategy: Australian Government, Department of Broadband Communications & the Digital Economy, 'The National Cloud Computing Strategy' (May 2013 accessed 17 June 2014) <www.communications.gov.au/__data/assets/pdf_file/0008/163844/National_Cloud_Computing_Strategy.PDF-289k-2013-07-21> In 2012, the EU adopted 'Unleashing the Potential of Cloud Computing in Europe' (2012): European Commission, 'Unleashing the Potential of Cloud Computing in Europe' Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions (27 Sept 2012 accessed 8 June 2014) <http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm.

[27] BSA The Software Alliance, '2013 BSA Global Cloud Computing Scorecard A Clear Path to Progress' *Gallexia Consulting* (2014 accessed 10 Aug 2014) <http://cloudscorecard.bsa.org/2013/index.html>.

[28] John Brunning, 'United Kingdom: The Consumer Cloud – A Cheap Alternative?' *Field Fisher Waterhouse* (3 February 2014 accessed 11 July 2014) <http://www.mondaq.com/x/290372/Consumer+Law/The+Consumer+Cloud+A+Cheap+Alternative>.

[29] See for example the recommendations of Eran Feigenbaum, Google director of Apps Security cited in Seth Rosenblatt 'Google, Microsoft agree: Cloud is now safe enough to use' *Cnet* (27 February 2014 accessed 7 July 2014) <http://www.cnet.com/au/news/google-microsoft-agree-cloud-is-now-safe-enough-to-use/>.

[30] Mainstream media articles are emerging which question certain practices of providers of free cloud services – see for example, the recent facebook case where they are alleged to have experimented with 689,003 users via their newsfeeds using a process called 'emotional contagion': Dan Swinhoe, 'Infoshot: Happy reading with Terms and Conditions (3 July 2014 accessed 27 July 2014) <http://www.idgconnect.com/abstract/8491/infoshot-happy-reading-with-terms-conditions> The published study confirms the assertion: Kramer, Adam, Jamie E. Guillory and Jeffrey T. Hancock, 'Experimental evidence of massive-scale emotional contagion through social networks' *Proceedings of the National Academy of Sciences* 111:24 [8788–8790] <http://www.pnas.org/content/111/24/8788.full> The ethics have been questioned and academics have referred the case to the Federal Trade Commission: Grimmelmann, James & Leslie Meltzer Henry, 'Letter to Edith Ramirez, Chairwoman Federal Trade Commission' (17 July 2014 accessed 2 Aug 2014) <http://james.grimmelmann.net/files/legal/facebook/FTC.pdf>.

[31] Mainstream media articles are emerging which question the practices of providers of free cloud services: Ibid. For empirical evidence, see Donald Robertson 'Cloud Computing Consumer Concerns Grow with use' *Research-ACMA Blog* (12 June 2013 accessed 11 July 2014) <http://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/researchacma/Cloud-computing-consumer-concerns-grow-with-use>.

[32] Note the comments in *Tech Republic* blog as to the closing Ubuntu One service: "Yes, it had its share of hiccups, but what service doesn't?" It is difficult to imagine a motor car reviewer writing a similar such remark; it seems that consumers are conditioned to expect product defects in computing and especially in terms of the cloud, which may affect the willingness of consumers to take legal action when products or services do not deliver: Wallen, Jack 'Ubuntu One falls from the clouds' *Tech Republic* (4 April 2014 accessed 30 Aug 2014) <http://www.techrepublic.com/article/ubuntu-one-falls-from-the-clouds/>.

[33] Brunning, above n 28.

[34] See above n 23 for the definition of SME.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

fit[35] – and nowhere is this seen more clearly than in consumer liability areas which are the focus here. Arguably, it is only now that cloud integrity in this sense is presenting as an impediment to wider uptake, that consumer law is being seriously considered to redress a perceived market failure,[36] and its potentials to reshape the industry from a consumer perspective are slowly emerging.[37]

Having now briefly outlined the context, the next section, **part 2,** briefly considers the commercial basis for the free cloud, defines the complex meanings of 'consumer' and the 'cloud', and then goes on to discuss the statistics of cloud use and awareness amongst both consumers and SMEs; **part 3** discusses barriers to cloud adoption, briefly looking at security issues before a more detailed consideration of standard form contractual issues; **part 4** looks at the application of the *Australian Consumer Law* with a brief comment as to other laws which potentially apply, and considers some recent 'cloudy' cases; **part 5** examines potential industry regulatory solutions, focussing on the NZ *CloudCode* and appraising its approach by reference to best practice, and then questions the adverse 'Australian' industry reaction to self-regulation; **part 6** looks beyond present regulatory structures to ask what other options might present and in conclusion, **part 7** reflects upon the state of consumer rights and understandings in cloud computing in Australia today – finding that the industry has significant risk assumption, contractual simplification and educative communication work yet to do to better encourage consumer- SME paid cloud uptake and more universal adoption.

2. About consumers & the cloud: definition(s) & up-take

Defining the 'cloud' is not as easy as one might expect. In a business context, it is often described as an "IT cost reduction lever"[38] but KPMG[39] says this is maturing into long term business objectives and strategic planning.[40] It seems clear that the extensive and growing large business uptake of private and hybrid cloud solutions suggests that for this decade of IT provisioning at least, cloud computing is the commercial ICT future of choice.[41]

In contrast, free consumer cloud services have already evidenced a capacity for "disruptive [social] innovation" as defined by Christensen.[42] Services such as *Google Apps, Dropbox, iCloud* and *Gmail* and international providers such as *Google, Amazon, Microsoft* and *Apple* are ubiquitous and are reshaping consumer communications in the twenty-first century.[43] Consumers enjoy a range of cloud offerings free in service areas as diverse as e-commerce, apps design, entertainment, social media, search and hardware,[44] funded by revenue streams such as advertising, subscription, lead generation, selling data, *freemium*[45] and

[35] For example, such as intellectual property, contract, privacy and competition laws. C/f Gasser, who argues that cloud computing and the legal and regulatory system interact "by identifying, clustering and analysing reactions by the legal and regulatory systems in response to the emergence of cloud computing". He suggests that the response is not a "simple stimulus-response mechanism" but a more complex interaction between different social forces and sub-systems, that there are "bi-directional feedback loops" between law and innovation and thirdly, that cloud computing has not emerged within a vacuum; that is, the legal and regulatory context has set the "enabling and constraining ground rules" just as it has always done for technological innovation: Gasser, above n 5.

[36] The specific market failure which the Government seem to be concentrating upon, is information asymmetry. There is little evidence of abuse of market power in the cloud industry. See the discussion in Australian Government, Department of Communications, 'Cloud Computing Regulatory Stocktake' Version 1 (May 2014 accessed 17 June 2014) [70] <http://www.communications.gov.au/__data/assets/pdf_file/0004/226930/Cloud_Computing_Regulatory_Stock_Take_-_May_2014.pdf>.

[37] While this may seem an odd proposition, there are NO cases consumer v. cloud provider as to the consumer cloud in Australia; the ACCC has foreshadowed its interest and awareness of some issues – but failed to really take any action or release educative materials at this stage. Cloud computing is being left to ACMA which has undertaken significant research but little consumer education and even less action against cloud service providers (as it only covers those which fall within its legislative regime). See the discussion in Part 5 below.

[38] The cloud has been seen an outsourcing IT and also, allows the transfer of IT across the balance sheet. KPMG International, 'Breaking through the Cloud Adoption Barriers' *KPMG Cloud Providers Survey* (March 2013 accessed 7 July 2014) [6] <https://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Documents/breaking-through-the-cloud-adoption-barriers.pdf> citing Rick Wright, Global Cloud Enablement Leader, KPMG. See also "a new lower cost form of outsourcing": Hagel, John & John Seely Brown, '4 Waves of Disruption: The Cloud – what it is, how it got here, and where it is going' *BSMReview* <http://www.bsmreview.com/cloudwaves.shtml>.

[39] The 2013 KPMG survey revealed 48% of business executives cited "cost reduction" as a key objective: Ibid: 6.

[40] Ibid.

[41] This view prevails both in government and corporate circles. However note the NAB and government departments report to the Australian Computer Society that many cloud offerings cannot meet their industry or internal compliance requirements as to security: Australian Computer Society, 'ACS Cloud Protocol Consultation' Report on the outcome of the ACS Public consultation on Cloud protocol (11 Nov 2013 accessed 6 July 2014) <http://www.acs.org.au/__data/assets/pdf_file/0017/27800/ACS-Cloud-Protocol-Consultation-Report.pdf>.

[42] Clayton M. Christensen, The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You Do Business (Collins Business Essentials) 2003 Put simply, this means an innovation which helps to create a new market and value network, and which eventually disrupts the existing market and displaces the earlier technology.

[43] Global Access Partners Pty Ltd, 'GAP Workshop on Cloud computing' *Report* (24 June 2011 accessed 11 July 2014) [6] <http://www.globalaccesspartners.org/GAP-Workshop-on-Cloud-Computing-Report.pdf>.

[44] Seer Interactive, 'How do they make money?' (2012 accessed 27 July 2014) <http://rcs.seerinteractive.com/money/>.

[45] This cloud service is free to the end-user (excluding use costs such as bandwidth) but is usually accompanied by subscription-based premium services. The other main model for cloud service revenue generation is 'pay per use' whereby end users pay for the service they use (plus costs such as bandwidth) as distinct from a license-based approach: Ibid.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

royalties.[46] But unlike commercial cloud offerings, the majority of consumer uptake involves *free* service use via internet access,[47] which indicates why the consumer cloud business model is so challenging for cloud providers. In 2014, *Juniper* report that cloud-based storage providers have achieved high volume use but are failing to capture paying subscribers,[48] which is forcing prices down - for example, *Ubuntu* recently withdrew from the cloud storage market, stating that "current price wars are 'unsustainable'."[49] A brief case study of the cloud digital music industry illustrates the problem. In 2003 Steve Jobs[50] told *Rolling Stone* that people want to own, not rent, their music:

> *... the subscription model of buying music is bankrupt. I think you could make available the Second Coming in a subscription model and it might not be successful.*[51]

Fast forward fifteen years, and Jobs seems vindicated, at least in terms of subscription as a revenue stream. Even for extremely popular high revenue music providers like *Spotify*,[52] profits are 'elusive'.[53] Publicly-listed *Pandora*[54] is valued at 5.48 billion dollars, has 76.4 million 'active' users[55] – but only three million paying subscribers[56] and by 2013 end, ran at an operating loss of $37 million.[57] The business stories for other popular cloud platforms are similar in terms of subscription as revenue. Advertising,[58] sale of participant data,[59] personalising user experience[60] and other revenue streams independent of user payment are therefore vital,[61] but justifiably exacerbate consumer concerns as to privacy, security and abuse of personal or business information provided or stored in the cloud.[62] Studies also show that the relatively low rate of SME uptake in Australia, compared with that of large business, is consistent with this more general consumer pattern. As Jobs said, people do not want to "pay", either for music by subscription – nor it seems, for their cloud services.[63]

It is important to define the ubiquitous terms 'consumer' and 'cloud' to better understand this 'free' versus paid differential and its implications for consumer cloud computing, practically and legally.

2.1. *Definition(s): 'consumer'*

The term 'consumer' has many nuanced meanings around the globe, especially in a cloud context.[64] In Australia, the

[46] Ibid.

[47] Stern Curator 'In praise of the consumer cloud' *WhaTech* (16 June 2014 accessed 11 July 2014) <http://www.whatech.com/cloud-computing/21744-bit425-in-praise-of-the-consumer-cloud>.

[48] Ibid citing Juniper, 'Cloud Computing – Consumer Markets: Strategies and forecasts 2014–2018'.

[49] Lawson, Stephen, 'Canonical shutters Ubuntu One music-streaming and cloud-storage service' *PC World* (2 April 2014 accessed 1 Aug 2014) <http://www.pcworld.com/article/2139120/canonical-to-close-ubuntu-one-cloudstorage-service.html> See also Stern Curator, above n 47.

[50] Of course Jobs had a contrary business agenda to sell, which was iTunes.

[51] Steve Jobs, 'The Rolling Stone Interview' *Rolling Stone Magazine* (3 Dec 2003 accessed 30 Aug 2014) http://www.keystonemac.com/pdfs/Steve_Jobs_Interview.pdf Note he was in the process of spruiking *iTunes* to industry executives.

[52] Spotify has 24 million active users, and is valued at $4 billion (2013): Loeb, Stephen 'How does Pandora make money?' *Vatornews* (21 Dec 2013 accessed 28 July 2014) <http://vator.tv/news/2013-12-21-how-does-pandora-make-money>.

[53] Above n 44 citing <on.mash.to/Q1WXSs, b.qr.ae/RZFoXg> See also Juniper, 'Cloud Computing – Consumer Markets: Strategies and forecasts 2014-2018' cited in Stern Curator, above n 47.

[54] Pandora describes itself as "free personalised internet radio": Pandora, 'What is Pandora' (undated accessed 28 July 2014) http://help.pandora.com/customer/portal/articles/182180-what-is-pandora It provides users with music streaming and recommendations based upon user preferences.

[55] It has over 250 million accounts. Paul Bonanos 'Pandora Beats Revenue Expectations, But Falls Short of Profit' *Billboard* (July 24, 2014 accessed 28 July 2014) <http://www.billboard.com/articles/news/6186141/pandora-earnings-call>.

[56] Subscription is to the Pandora One service, which costs $3.99 a month.

[57] In 2014, Pandora's revenue was $180 million in the third quarter, of which 80% or $144 million, was advertising revenue and (mostly) subscription (20%): Loeb, above n 52. Pandora's revenuewas $4.18 million (2007): Statista, 'Pandora's revenue from 2006 to 2013, by source (in USD million)' (2014 accessed 28 July 2014) http://www.statista.com/statistics/190918/revenue-sources-of-pandora-since-2007/. In 2014, Pandora has just revised revenue expectations upward from $895 million to $915 million: Bonanos, above n 52. Even after a share price dip on recent quarterly results, this is a share multiple of around 5× revenue.

[58] Facebook has "sponsored" (i.e. paid) advertisements, which it targets to user interests.

[59] User data may be either profiled to enable targeted advertising or anonymised for sale to data aggregators.

[60] For example, Apple iCloud analyses user information for this purpose.

[61] ACMA, 'The cloud: services, computing and digital data—Emerging issues in media and communications, Occasional paper 3' (June 2013 accessed 11 July 2014) [8] <http://www.acma.gov.au/~/media/Regulatory%20Frameworks/pdf/The%20cloud%20services%20computing%20and%20digital%20data%20Emerging%20issues%20in%20media%20and%20communications.pdf>.

[62] Heather Kelly, 'Why Gmail and other e-mail services aren't really free' *CNN* (1 April 2014 accessed 28 June 2014) http://edition.cnn.com/2014/03/31/tech/web/gmail-privacy-problems/index.html?iid=EL "'The basic premise of Gmail is, we'll give you a robust e-mail service and in exchange we want to display ads alongside our e-mail and we're scanning your e-mail to decide what ads are most relevant,' said Eric Goldman, a professor at the Santa Clara University School of Law.".

[63] ACMA, above n 61: 10.

[64] See for example Martin Ebers 'The Notion of Consumer in Community Law' *Comparative Analysis* (undated accessed 10 Aug 2014) <http://www.eu-consumer-law.org/consumerstudy_part3a_en.pdf>; Kingisepp, Margus and Age Värv, 'The Notion of Consumer in EU Consumer Acquis and the Consumer Rights Directive—a Significant Change of Paradigm?' *Juridica International* (2011) XVIII <http://www.juridicainternational.eu/?id=14841 accessed 10 Aug 2014>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

prevailing consumer law[65] definition is in the *Australian Consumer Law* ('ACL').[66] The term 'consumer'[67] is used in several ACL provisions only, but mostly, the Act covers both individuals and SME businesses.[68] For example, consumers often benefit under ACL provisions proscribing supplier misleading and deceptive conduct,[69] unconscionability[70] and false representations[71] – albeit not specifically referred to per se. The two relevant sections which refer to 'consumer'[72] are Part 3-2 consumer guarantees and 'consumer contract' in the unfair contract terms regime in Part 2-3.

Under Section 3 of the *ACL*, an acquiring entity is presumed a "consumer" if the price[73] of goods or services acquired[74] is $40,000 or less; or alternatively, the goods[75] or services[76] (objectively assessed)[77] are of a kind ordinarily acquired for 'personal domestic or household use or consumption',[78] subject only to limited use exclusions for goods.[79] There seems little doubt given the ubiquity of home computing that cloud computing is of the "kind" of good or service contemplated. However, goods'[80] are defined to include 'computer software' which clarified previous uncertainty as to whether software downloaded over the internet falls within the ACL.[81] Whether *SaaS* is a 'good' or 'service' is perhaps not beyond doubt, despite the definition. Arguably, it seems a step further away from direct software download, insofar as it is usually accompanied by ongoing services by the provider and is not physically stored on a consumer's hard drive. There is no Australian case decided on the point to date and it seems open for this mode of software provision to constitute a 'service' rather than just 'goods' – but a court may find it to be a matter of degree in terms of the specific offering on a case by case basis. It seems likely that all other cloud services – *PaaS* and *IaaS* – would constitute 'services' under the ACL too. 'Services' include rights, benefits or privileges or facilities to be provided, granted or conferred under "… a contract for or in relation to the performance of work … whether with or without the supply of goods …"[82] This discussion continues in Part 4 below when consumer guarantees are looked at in greater detail. It should also be noted that many cloud 'acquisitions' are essentially a license by subscription and while there is no authority on this point, the inclusive definition of "acquire"[83] under the *ACL* seems broad enough to include this concept. In summary, cloud computing acquisitions seem likely to fall within the ambit of the *ACL* definitions in most instances due either to the quantum involved or the fact that cloud services are of the type which people ordinarily use in a personal, domestic or household computing context. In the latter situation, a court will examine the specific facts of each case, and it may be that certain types of cloud provisioning over $40,000 may be deemed a "consumer" transaction such that businesses are covered by the *ACL*, whereas other types, potentially, may not.[84]

In contrast, Part 2-3 unfair contract terms provisions apply only to a "consumer contract" which is defined as a supply of

[65] Note that the ACL does not apply to the supply of financial services or products: *Competition & Consumer Act 2010* (Cth) s131A except for linked credit provider provisions under ss 278–287. Equivalent provisions apply as to financial services and products in Div. 2 Part 2 of the *Australian Securities and Investments Commission Act 2001* (the ASIC Act).

[66] Schedule 2 of the *Competition and Consumer Act 2010* (Cth).

[67] Section 3 (1)(a)(i) of the *Australian Consumer Law* states a person is taken to have acquired goods as a 'consumer' if the cost is $40,000 or less, or where greater (b) the goods were of a kind ordinarily acquired for personal, *domestic or household use or consumption*; (c) … consisted of a vehicle or trailer acquired for use principally in the transport of goods on public roads. The definition excludes acquisitions for the purpose of: (a) … re-supply; (b) … using them up or transforming them, in trade or commerce (as defined); or (i) in the course of a process of production or manufacture; or (ii) in the course of repairing or treating other goods or fixtures on land. Goods are defined to include 'software': section 2(e) and 'consumer contracts' are defined in section 23(3). "Services" are acquired as a consumer if they cost $40,000 or less, or are of a kind ordinarily acquired for 'personal, domestic or household use or consumption'.

[68] SMEs are defined above n 23.

[69] ACL Part 2-1.

[70] ACL Part 2-2.

[71] ACL Part 3-1.

[72] The ACL also defines 'consumer goods' under Parts 3-3 and 4-3 in the context of product safety standards.

[73] See sections 3 (4)–(9) as to the calculation of the "amount paid or payable".

[74] 'acquired' or 'to be acquired' is the language of the section.

[75] ACL section 3(1).

[76] ACL Section 3(3).

[77] The 'objective' assessment means that goods such as commercial grade insulation, commercial alarm systems and commercial grade carpet have been found to be consumer purchases, albeit purchased by businesses for commercial premises and uses. See *Bunnings v Laminex* [2006] FCA 682), *Crawford v Mayne Nickless Ltd* (1992) ASC 56-144; (1992) ATPR(digest) 46-091 and *Carpet Call v Chan* (1987) ASC 55- 553; (1987) ATPR (Digest) 46-025 respectively. In that latter case, the court said that carpet does not lose its character as a personal, domestic or household item, by reason of any 'commercial' quality. Likewise inherently commercial products or services do not become a consumer item just because their (subjective) use is of a personal domestic or household nature: examples include a large tractor (*Atkinson v Hastings Deering (Qld) Pty Ltd* (1985) 8 FCR 481; 71 ALR 93).

[78] This definition is similar to that in section 4B of the *Competition and Consumer Act 2010* (Cth).

[79] The exclusions in section 3 relate to the acquisition or holding out as acquiring, goods for the purpose of resupply, using them up or transforming them in trade or commerce, or in the process of manufacture or production or the treating or repair of other goods or fixtures on land. This exclusion seems unlikely to apply in most cloud computing scenarios and so is not considered further in this paper.

[80] The definition of 'services' in s 2 of the ACL, is substantially similar to the definition in s 4 of the CCA. As to 'goods' section 2 added new inclusions: computer software, second-hand goods and any component part or accessory to, goods.

[81] Prior to the clarification, there was doubt as to whether unboxed software would constitute a 'good': *Amlink Technologies Pty Ltd and the Australian Trade Commission* (2005) AATA 359. As pointed out by Forder & Svantesson, Forder, Jay & Dan Svantesson, *Internet & Ecommerce Law* (Oxford University Press, 2010) [87] there can be little rationale for a consumer-protection distinction between software purchased from a shop and software purchased online.

[82] ACL section 2.

[83] 'acquire' includes (a) in relation to goods – acquire by way of purchase, exchange or taking on lease, on hire or hire purchase; and (b) in relation to services – accept: ACL section 2. Under section 11 references to acquisition … include.

[84] In that situation, a business would have recourse to the contract as between it and the cloud services provider to ascertain a basis for liability, as well as general law.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

goods or services[85] … "to an individual, whose acquisition … is [subjectively] wholly or predominantly for personal, domestic or household use or consumption".[86] Incorporated small business cannot therefore utilise the unfair term provisions to cover impending amendments (though this is to change this shortly). It is however possible that an unincorporated sole trader, for example, might purchase goods or services for an acquisition which is predominantly for personal, domestic or household use or consumption, even if partly for business purposes.[87] The federal government is currently enquiring into extending section 23 to include small business.[88]

In summary, it seems likely that the majority of consumers and businesses in Australia acquiring cloud goods or services are covered under the *ACL* – except for SMEs under the unfair terms regime in section 23. These laws are discussed further under part four below.

2.2. *Definition(s)*[89]*: 'cloud computing'*

The ACL provides that a consumer is not just a private individual but includes businesses in certain legal contexts, so the next question is what are those contexts within cloud computing; that is, what is the "cloud" and how do consumers potentially use it?

Cloud computing may be broadly defined as the internet-enabled "consumption of information and communications technology".[90] In simple terms, it is analogous to leasing[91] or renting,[92] rather than buying, IT goods and services.[93] Consumer group ACCAL define cloud computing as "… storing and accessing data, programs and services over the internet rather than from your computer hard drive or server located on your [business] premises."[94] The generally-accepted industry definition[95] is that of the US National Institute of Standards and Technology ('NIST')[96] which the NZ *CloudCode* expressly incorporates and summarises as follows:

> … *on demand scalable resources such as networks, servers and applications which are provided as a service, are accessible by the end user and can be rapidly provisioned and released with minimal effort or service provider interaction …*[97]

Given its relative simplicity,[98] recent origin and industry-based formulation, this paper adopts this *CloudCode* approach. This includes the NIST definition reference to features such as cloud service model[99] and mode of deployment. Briefly, the models are as follows: Software as a Service (*SaaS*),[100] Platform as a Service (*PaaS*)[101] and Infrastructure as a

[85] Or the sale or grant of an interest in land, which is obviously irrelevant for the purposes of this paper.

[86] ACL section 23(3).

[87] Australian Government Solicitor, 'Australian Consumer Law' *Fact Sheet No. 12* (March 2011 accessed 28 June 2014) <http://www.ags.gov.au/publications/fact-sheets/Fact_sheet_No_12.pdf>.

[88] Consumer Affairs Australia and New Zealand, 'Extending Unfair Contract Term Protections to Small Businesses. Consultation paper' Department of Treasury (May 2014 accessed 14 July 2014) http://www.treasury.gov.au/ConsultationsandReviews/Consultations/2014/~/media/E53165D4D8B24B4799395680E68FE0B0.ashx.

[89] "Cloud computing will never have a universally agreed-on view and definition … [e]ven attempts to classify it … and to evolve with real-world usage (e.g. hybrid) are actually causing more, not less, confusion.": Gartner, 'Predicts 2013' (4 Dec 2012 accessed 17 June 2014) https://www.gartner.com/doc/2263916?ref=SiteSearch&sthkw=cloud%20computing&fnl=search&srcId=1-3478922254#a-1819766141.

[90] Above n 35.

[91] This term appears in the recent National Commission of Audit Report, Recommendation 63: "Cloud computing is a way of leasing computing services over a network": National Commission of Audit, *Towards Responsible Government: Report Vol 1* (Feb 2014 accessed 2 Aug 2014) <http://www.ncoa.gov.au/report/index.html>.

[92] Neither leasing nor renting are foreign concepts to Australian consumers, who habitually rent whitegoods, computing equipment and the like both for small business and home use. Consumer and contract law generally regulate cloud computing contracts and related industry conduct as to supplies of goods and services, whether by hire, sale or lease.

[93] Queensland Government, 'Cloud computing for business' (22 May 2014 accessed 7 June 2014) http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business.

[94] ACCAN, 'How to choose a cloud computing provider' *Tip Sheet* (undated, accessed 17 June 2014) http://www.accan.org.au/consumer-info/small-business/small-business-tip-sheets/801-how-to-choose-a-cloud-computing-provider.

[95] Note that the Australian Government share the Gartner perspective when it reports "even ICT specialists do not share a common definition of cloud computing": Regulatory Stocktake above n 36:13.

[96] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction …": NIST, above n 9.

[97] ACCAN, above n 94: 3.

[98] One Harvard paper suggests the following: "… multi-faceted technological phenomenon in which important aspects of computing (such as information processing, communication, networking, data acquisition, storage, and analysis) move from local systems to more efficient, outsourced systems where third parties provide aggregated computational resources and services on an as-needed basis from remote locations": Urs Gasser, above n 5.

[99] A non-technical description of these models is found in Skytap Blog, 'Demystifying SaaS, PaaS, and IaaS' *Skytap* (21 July 2011 accessed 29 July 2014) <http://www.skytap.com/blog/demystifying-saas-paas-and-iaas>.

[100] *SaaS* is the most common form of cloud computing adopted by SMEs and allows access to software applications via a browser, without the need for a consumer to load software on either a PC or server. The *SaaS* provider usually controls and maintains the application, including updates and settings. Examples include Hotmail, Instagram and flickr.

[101] *PaaS* is the "provision of computing platforms to create an environment for other software to run (e.g. operating systems) over a network, rather than being loaded directly onto a locally available computer": Australian Government Information Management Office, 'Negotiating the Cloud – Legal Issues in Cloud Computing Agreements Better Practice Guide' *Department of Finance and Deregulation* (Feb 2013 accessed 26 July 2014) [4] <http://www.finance.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf> Examples of *PaaS* providers include Google App Engine, VMWare's Cloud Foundry and OpenShift (by Red Hat). IDC estimates the $3.8 billion (2012) *PaaS* market will grow to $14 billion by 2017: Burke, Steven, 'The 20 Coolest Cloud Platforms and Development Vendors Of The 2014 Cloud 100' (30 Jan 2014 accessed 21 July 2014) <http://www.crn.com/slide-shows/cloud/240165700/the-20-coolest-cloud-platforms-and-development-vendors-of-the-2014-cloud-100.htm>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

Service (*IaaS*).[102] The second feature – mode of deployment – entails four models: private,[103] community,[104] hybrid[105] and public.[106] Rather than defining these models and modes of deployment, see the descriptive KPMG table at Annexure One.

2.3. *Awareness, prevalence & use*

Consumer uptake of cloud computing is significant and escalating.[107] In 2013, internationally, it is estimated that over 2.4 billion 'unique' consumers accessed cloud-based services, a figure predicted to increase to over 3.6 billion consumers by 2018.[108]

In Australia, surveys suggest that eighty percent of adults[109] – 14 million people – used cloud computing in the six month period to May 2013,[110] predominantly via webmail services (88%) and cloud-based software (40%).[111] This represents a significant (11%) increase for the same period in 2012. Similarly consumer use of portable devices such as smartphones and tablets, which enable consumer cloud uptake, is exponentially on the rise.[112] Fuelled by multiple portable devices, games, music and social media, consumers continue to represent a significant potential growth market for cloud computing. In contrast, statistics suggest that SME consumers in Australia are relatively 'slow' to adapt to cloud computing, an issue which has generated significant economic policy concern from the (former) federal government,[113] industry groups[114] and independent public policy bodies.[115] A 2013 MYOB Study found only 16% of SMEs[116] are using cloud computing,[117] though those 'users' were 106% more likely to benefit through increased revenue over the next year as a result. The study also found that 35% of SMEs reject cloud computing options due to a lack of knowledge about cloud services.[118] A smaller ACMA study found higher levels of SME cloud up-take, finding that 44% or approximately 900,000 Australian businesses had actively used cloud computing services as at May 2013.[119]

It seems possible that as individual consumer statistics suggest, many small businesses may not realise that they are cloud users already. *Sensis* (2014) ask very specific questions which give examples of popular platforms[120] and show that 37% of SMEs have a cloud-based social media presence[121] whereas almost 80% of large businesses do.[122] Of those SMEs who don't, 19% "intend to do so" in the next year,[123] a figure which perhaps supports the fact that most owner/managers run small business social media[124] and barriers as to time, a lack of confidence, ignorance, security concerns and so on, remain significant.[125] ACMA research supports this view;

[102] *IaaS* refers to the external provision of both computer hardware and disk space (essentially processing capability and data storage)[103] which is accessible by the internet or through a private network: AGIMO, Ibid. Examples include Rackspace, Amazon EC2, Google Compute Engine, HP Cloud & Microsoft Windows Azure. Amazon is by far the largest provider of such services, which Gartner estimate were valued at $9 billion worldwide in 2013: Kristin Bent, 'The 20 Coolest Cloud Infrastructure, IaaS Vendors Of The 2014 Cloud 100' *CRN The Channel Company* (31 Jan 2014 accessed 21 July 2014) <http://www.crn.com/slide-shows/cloud/240165705/the-20-coolest-cloud-infrastructure-iaas-vendors-of-the-2014-cloud-100.htm/pgno/0/1>.

[103] A 'private' cloud is a dedicated cloud which restricts access to one entity and is therefore the highest security offering; it is the most common form of business cloud computing in Australia. Some analysts exclude private deployment, arguing that the cloud presupposes a "shared utility" KPMG, above n 24: 9.

[104] 'Community' clouds offer access to a specific community of entities (for example, government departments).

[105] 'Hybrid' clouds generally feature two or more deployment models operating in tandem with a level of interactivity which is not otherwise available between clouds.

[106] A 'public' cloud is one with open access to all.

[107] ACMA, above n 61.

[108] Juniper Research, 'Consumer Cloud – There's No Limit' *White Paper* (2014 accessed 6 July 2014) <http://www.juniperresearch.com/shop/download_whitepaper.php?whitepaper=261>.

[109] The exclusion of the tech literate and dependent under 18 age bracket suggests that this figure may well be a significant underestimate.

[110] ACMA, 'Report 2 – Cloud Computing in Australia' *Communications Report Series* (March 2014 accessed 1 July 2014) [1] <http://www.acma.gov.au/~/media/Communications%20Analysis/Report/pdf/Cloud%20Computing%20.report_final%20pdf.pdf>.

[111] Ibid.

[112] In 2013, ACMA reported that as at May 2012, there were 8.67 million Australian adults with a smartphone, a 104% increase on the previous year: ACMA, 'Communications Report 3 – Smartphone and tablets: Take-up and use in Australia' *Summary Report* (2012) http://www.acma.gov.au/webwr/_assets/main/lib310665/report-3-smartphones_tablets-summary.pdf Smartphones and tablets are innately cloud-dependent as they are designed for portable use but have very limited storage: "Without a cloud storage service, the ability to share and work with saved documents becomes a logistical nightmare.": Wallen above n 32.

[113] Above n 26.

[114] Australian Industry Group, 'Australian Industry Group Submission to Australian Computer Society' (6 Sept 213 accessed 6 June 2014) <http://www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol/2013-australian-cloud-protocol-submissions>.

[115] Minifie, above n 22. This report did not include consultation with consumer groups.

[116] Note this definition *excludes* the not for profit sector. The Federal Government reports that there is limited data as to cloud computing up-take in this group:Regulatory Stocktake' above n 36.

[117] MYOB, *Business Monitor*, myob.com.au/myob/news-1258090872838?articleId=1257830858409, March 2013. The study reviewed over 1000 Australian SMEs.

[118] Ibid.

[119] ACMA, above n 23: 2.

[120] *Q. Does your business have a social media presence? This might include having a Facebook page, being active on Twitter, MySpace or LinkedIn, having a blog, hosting forums or having a social media based rating system?* Sensis, 'Yellow Social Media Report' (2014 accessed 29 July 2014) [59] <http://about.sensis.com.au/IgnitionSuite/uploads/docs/Yellow-Social-Media-Report-2014.pdf>.

[121] Sensis, ibid 61. This has risen each year from 15% in 2011. Interestingly the highest state use rate is in Queensland (48%) and regional use (40%) exceeds metropolitan (35%).

[122] The favoured social networks are (citing figures small: medium: large), facebook 82:89:83, twitter 25:37:61, LinkedIn 25:17:37, Google+ 11:9:24 and youtube 7:9:28, instagram 5:9:24, pinterest 4:7:14, blog 4:6:7, yammer 0:0:2: Sensis, Ibid.

[123] Ibid: 60.

[124] Ibid: 66.

[125] Of consumers who had heard of cloud computing 38% thought they were cloud users whereas actually 90% were. Of those who had not heard of cloud computing, 65% were using a cloud service: ACMA, Ibid: 17. [same n as 35].

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

suggesting that active usage[126] far exceeds awareness[127] levels. The report estimates that while 55% of those surveyed had 'heard' of cloud computing, only 26% of users realised they were using the cloud.[128] Interestingly, the most commonly-used SME services mirror those used by individual consumers – webmail (57%) and file-sharing (43%)[129] – which may also suggest that SME usage is no more business-oriented or commercially informed than that of individual users or perhaps, leverages off individual user experience, knowledge and/or preference.[130]

In terms of consumer perception as to benefits of cloud computing, ACMA report cloud consumers cite multi-device access (43%),[131] backup security (33%) and additional storage (19%) as the main benefits, whilst perceived negatives were a lack of security (52%), mistrust in cloud services providers (14%) and reliability concerns (12%). SME responses were quite similar: ease/convenience of use (36%), multiple platform (15%), back-up in the event of computer network failure (11%) all featured, but surprisingly, over 20% claimed ignorance[132] ('don't know') as to cloud benefits. Of those non-user SME's, the main reason was that the respondent did not regard cloud services to be 'suited to their business' (48%) and 22% indicated they did not know enough about cloud computing.[133]

It is worth concluding with the federal government's approach to the cloud given its potentials to influence SME uptake. Despite significant investment in cloud strategies,[134] government cloud uptake performance is poor. The 2014 Commission of Audit (CoA) states:

> *A reliance on bespoke, legacy systems, concerns about the security and privacy of placing public data in the cloud, and general risk aversion all impede progress …* [135]

The federal government spends around AU$6 billion a year on ICT of which less than $5 million has been spent on cloud services since July 2010.[136] In July 2014, the current Australian Government has recommitted[137] to a 'cloud-first' policy for federal government agencies consistent with recent recommendations of the CoA.[138] In October 2014, the Government issued a revised policy of e-government and the digital economy,[139] specifying 'cloud first' - subject to the significant (and potentially subjective) criteria of it being fit for purpose, providing adequate data protection and value for money.

3. Oh, but the cloud has 'issues'

> *With the cloud, you don't own anything. You already signed it away … The more we transfer everything onto the Web, onto the cloud, the less we're going to have control over it…*
>
> Steve Wozniak.

[126] ACMA, above n 23: 19. In the six months to May 2013, consumer cloud-based activities were as follows: 12.2 million use webmail (e.g. hotmail gmail, yahoo!7 mail) which represents 88% of all cloud users, 9.8 million used social networks (e.g. facebook, linkedin), 7.2 million store of personal photos, 6.1 million used Apps (Google documents or adobe photoshop express), 2.2 million stored personal videos online, 1.7 million backed-up their hard drive online and 1.4 million used paid file storage. It is important to note however that the exclusion of users under 18 years may be significant in consumer-user statistics, given the widespread social media and growing cloud usage by younger Australians.

[127] ACMA above n 23: 2. Awareness increased with income levels – up to 77% for people earning at or above $130,000 per annum – and peaked at 69 per cent for those age 35–44 (69%) down to a low of 33% for those aged 65 years plus.

[128] This suggestion is made as the ACMA survey did not ask respondents if they had used "cloud services" per se; it specifically itemised "… webmail, streamed content online backed-up and stored files online and shared files online" rather than relying upon consumer awareness as to what constituted a 'cloud' service: Ibid 17 footnote 1.

[129] ACMA above n 31 [2].

[130] Of course it may also suggest that these services are the ones of greatest utility to SMEs or that other factors apply – there appears to be no specific research to determine the question.

[131] Devices consumers used were laptops (59%), mobile phone (57%), PC (52%) and tablet (47%): ACMA, above n 23: 38.

[132] ACMA, above n. 23: 21.

[133] ACMA, above n. 23: 22.

[134] Above n 26.

[135] The National Commission of Audit Report 2014 cited in Chris Duckett, 'Government needs to move online quicker: Commission of Audit' (1 May 2014 accessed 2 Aug 2014) <http://www.zdnet.com/government-needsto-move-online-quicker-commission-of-audit-7000028969/>.

[136] Minister for Communications, Malcolm Turnbull MP cited in Josh Taylor 'Australian government revises cloud computing policy' *ZDNet* (31 July 2014 accessed 2 Aug 2014)< http://www.zdnet.com/australian-tech-sector-growth-outpacing-us-uk-report-7000032180/> Asian-Pacific cloud computing revenue is AUD$5, 267 million (2013) with growth projections to AUD$19,910 million by 2020 (figures converted from euro): Statista, 'Projected revenue of cloud computing in the Asia/Pacific region from 2008 to 2020 (in million euros)' (2014 accessed 28 July 2014 <http://www.statista.com/statistics/270817/projected-cloud-computing-revenue-in-asia-since-2008/>.

[137] The present government's 2013 election policy was less enthusiastic, indicating that smaller agencies would use shared or cloud services where efficiencies could be evidenced, and that there would be a "trial" to test relocating critical government data to a secure government cloud by 2014. This has not yet eventuated and may be overtaken by a revised cloud computing policy, to be announced later in 2014.

[138] Recommendation 63: Cloud computing provides that "Cloud computing is a way of leasing computing services over a network. It can reduce costs by sharing them across users. The Commission recommends that the Government increase its adoption of cloud computing by: (a) introducing a mandatory 'cloud first' policy for all low risk, generic information and communication technology services; and (b) establishing a whole-of-government cloud computing provider panel: National Commission of Audit, *Towards Responsible Government Report* (2014 accessed 2 Aug 2014) <http://www.ncoa.gov.au/report/index.html> See also AAP 'Australian tech sector growth outpacing US, UK: report' *ZDNet* (31 July 2014 accessed 2 Aug 2014) <http://www.zdnet.com/australian-tech-sector-growth-outpacing-us-uk-report-7000032180/>.

[139] See Taylor, above n 136. The policy can be seen here: Australian Government. 'Cloud Computing Policy v 3.0 Oct 2014' (Oct 2014, accessed 5 March 2015) <http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

That the government has been slow to adopt paid cloud computing and free-use consumers exponentially fast, is an interesting reflection upon relative perceptions of cost, risk, privacy and security. While not purporting to discuss these topics in any depth, a brief overview of barriers to cloud uptake and security issues is useful as a background to considering cloud computing contract terms and conditions.

3.1. Barriers to consumer cloud adoption

In May 2013, the *National Cloud Computing Strategy* provided that Australian consumers and small business will be provided with the tools and protections required to enable cloud use with confidence. ACMA report that consumer confidence and trust concerns present three main barriers: firstly, security, privacy and data management; secondly, vendor lock-in, interoperability and portability between cloud services with consequent loss of control over personal or business data; and finally, data sovereignty[140] and concerns as to inadequate redress mechanisms.[141] The data suggests that 52% of Australians lack confidence in privacy settings for online services[142] and over two thirds are concerned about unauthorised use of personal information and security generally.[143] Only 8% pay to store their data online which ACMA claim evidences "explicit decisions to limit their cloud activity".[144] Further, cloud terms and conditions of service evidence tensions between consumer expectation and cloud industry practices as discussed in part 3.3 below.[145] Industry proprietary standards and service agreements also recognise that data may not be transferable between different services for technical reasons, which impacts greatly upon cloud convenience and practicality. Consumers risk becoming technically locked-in to a specific vendor, which inhibits choice, raises the risk of lost content and adversely impacts upon competition within the marketplace.

Finally, although the Australian-based market is growing,[146] many cloud providers are located overseas which raises a host of legal and enforcement issues in the event of privacy or data breach, contractual dispute or otherwise – in particular, the questions of jurisdiction, choice of law and enforcement cost. ACMA report that 35% of Australians would withhold personal information to overseas providers out of security concerns, and assert that this is an issue for consumers and businesses,[147] especially with public cloud providers, the majority of whom are located overseas.

3.2. Major (very public) security breaches

Public and potentially serious cloud security breaches have affected most major online platforms, from twitter[148] to dropbox,[149] Facebook, Apple iCloud,[150] Google Apps and Gmail.[151] Since 2012, Amazon, Microsoft Office 365, Outlook.com, Bing, Azure Cloud, Xbox, Cloud fare (taking more than 750,000 other sites with it - including *Wikileaks*), Outlook.com mail, Amazon (Pinterest, Netflix, instagram) have all suffered outages affecting millions of users worldwide. The causes of

[140] Data sovereignty refers to consumer/SME data ownership and access where data is stored overseas.

[141] ACMA above n 61.

[142] ACMA above n 61: 15 (footnote 24) citing ACMA, 'Digital Footprints & Digital identities – Community Research' (2013) unpublished.

[143] ACMA, 'Report 2 – Australia's Progress in the Digital Economy: Participation Trust and Confidence' (2012 accessed 13 July 2014) [25] <http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.acma.gov.au%2Fwebwr%2F_assets%2Fmain%2Flib310665%2Faustralia's%2520progress%2520in%2520the%2520digital%2520economy.pdf&ei=JIDhU7iUCdjk8AXT4YDYBg&usg=AFQjCNHYfBIlYoFKLRJ7ipy7NDFYob7q3A&bvm=bv.72197243,d.dGc>.

[144] ACMA above n 61: 16.

[145] ACMA above n 61: 16.

[146] In 2013, there were 38 cloud service providers located in Australia via locally-based servers (e.g. Microsoft) or data centres (e.g. Amazon, Rackspace, IBM, Dell and Hewlett Packard): ACMA above n 61: 7.

[147] KPMG, 'Cloud Computing: Australian lessons and experiences' [14] cited in ACMA above n 61: 17 fn 23.

[148] An employee's email was hacked into, then the corporate Google Apps system accessed, which enabled the theft and publication of sensitive company documents. "This has nothing to do with cloud computing," said Sam Masiello, vice president of information security at Englewood, Colo.-based MX Logic. "It's about weak passwords that are easily guessable, with a huge contribution from people's habit of putting online information that they wouldn't otherwise share with anyone but their closest friends. It's not hard to crack [password resets] with the information you can find freely available on social networking sites." Keizer, Gregg 'Hacker break-in of Twitter e-mail yields secret docs' *Computerworld* (16 July 2009 accessed 30 July 2014).

[149] An employee's account was hacked enabling access into a dropbox account with the same password - The hacker then stole documents with user details and proceeded to send them spam; but could just have easily sent a phishing message to steal passwords or containing a link with malware. The incident was blamed upon "a single end-user's ignorance (or naiveté, if you prefer) about basic password security – possibly coupled with unclear or nonexistent data-security policies." Ted Samson, 'Dropbox fiasco serves as reminder of cloud-storage insecurity' *Infoworld (2 Aug 2012 accessed 30 July 2014)* http://www.infoworld.com/t/cloud-security/dropbox-fiasco-serves-reminder-of-cloud-storage-insecurity-199197 See also InfoWorld, 'Popular cloud sync app raises security fears' *Tech Watch (8 Nov 2011 accessed 30 July 2014)* <http://www.infoworld.com/print/157776>.

[150] Chris Griffith, 'Malware cripples Australian Apple iCloud accounts' The Australian (29 May 2014 accessed 29 July 2014) <http://www.theaustralian.com.au/technology/malware-cripples-australian-apple-icloud-accounts/story-e6frgakx-1226935680356> Users were advised to change their passwords and not to pay a ransom demanded when malware, locked apple users out in Australia. Users were also told to disable LostMode which was suspected to have been implicated in the problem. See also *Wired* reporter Matt Honan was hacked and his macbook air, ipad and iphone data was remotely wiped. The hacker had bypassed the security questions so an Apple employee reset his iCloud password: Samson, above n 149: 108.

[151] Gmail users have experienced over a dozen outages since the service became generally available in 2009. The most serious involved 1.5 million users (27–28 Feb 2011), 5.25 million users (17 April 2012) 'less than half' (Sept 2013_ which means over 200 million users and "most" users (24 Jan 2014). This latter case affected 'most' of 500 million users: Adrian, Covert, 'Gmail at 10: How Google dominated e-mail' *CNNTech* (1 April 2014 accessed 28 June 2014) <http://money.cnn.com/2014/04/01/technology/gmail>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

these outages may be technical but are not always disclosed, and may also be attack-based. *Alert Logic* report that cloud attacks are increasing across all incident types[152] and taking the recent *Heartbleed* virus as an example, one third of cloud services – including Yahoo – were vulnerable.[153]

Despite the absence of mandatory data breach disclosure laws in Australia,[154] which means the problem may be far larger than the mainstream media disclose, consumers know about it. Whether through media, blogs or private experience,[155] consumers are aware of the potential privacy and business costs that outages or other security problems may entail. A 2012 international report estimated, based on 13 cloud provider's press releases, that the average downtime between 2007 and 2012 was 7.5 h per year.[156] Time and costs are commercially (and privately) significant: for example, in January 2013 Amazon's home page was down for an hour which reportedly cost Amazon $5 million in revenue loss, then in 2013, Amazon's cloud servers were hacked which exposed "hundreds of thousands" of *LinkedIn* member profiles to cyber criminals. Estimates suggest that the average annual cost of cloud downtime to a fortune 500 company is $46 million and predict that 40% of companies will have lost cloud data within two to five years.[157] The cost to the financial sector and consumers of having private data stolen is likewise potentially catastrophic.

Industry explanations for these expensive events are rarely comforting; it does not generally seem adept at public disclosure and even where it occurs, it matters little to a consumer whose data has been stolen for a cloud provider to blame a stolen laptop or their own employee who had lax password security.[158] Inadequate industry corporate compliance and staff training is a data loss risk, just as much as that posed by cloud outages. And the providers are of course, responsible for both. Perhaps as one commentator remarked, the bigger picture really is that "… storing sensitive, unencrypted information in the cloud is foolish, no matter how you slice it."[159]

3.3. *Contractual nightmares: reading the terms and conditions*

The truth comes out when you begin discussing a contract.[160]

Online contracting is the burgeoning consumer law phenomenon of the twenty-first century.[161] It pervades all aspects

[152] The volume and persistence of attacks is increasing and those which were once directed at on-premise environments are "moving to the cloud". Alert Logic, Cloud Security Report (Spring 2014 accessed 10 July 2014) [12] <http://www.findwhitepapers.com/force-download.php?id=37838>.

[153] James Bourne ' One in three cloud services was susceptible to Heartbleed, research shows' *Cloudtech* (12 May 2014 accessed 7 June 2014) <http://www.cloudcomputing-news.net/news/2014/may/12/one-three-cloud-services-was-susceptible-heartbleed-research-shows/> The *Cloud Adoption & Risk* report cited found that 1173 of 3571 cloud services in use were exposed to Heartbleed, but that after a week, only 1% remained vulnerable. Heartbleed was labeled "extremely serious" and using it, security bloggers were able to access 200 user names and passwords for Yahoo mail within 5 min.

[154] There is no specific breach notification requirement across the EU/EEA (though see the *Privacy and Electronic Communications Directive* re electronic communications providers and ISPs), there are four states (2012-13) who have mandatory disclosure and Mexico, UAE, most of the USA all mandate disclosure. In Australia, *Guidelines* encourage the reporting of significant security breaches to the Office of the Australian Information Commissioner (OAIC) and individuals should be notified where the breach threatens a "real risk of serious harm": OAIC, 'Guide to handling personal information security breaches' (2008 accessed 29 July 2014) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches> In this non-mandatory guide, **data breach** means "when personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse." It does not apply to individuals or generally, SMEs – **"Organisation** … includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers and a limited range of small businesses (see ss 6C, 6D and 6E of the Privacy Act).".

[155] Recent events (2014) involving Apple iCloud and eBay Inc. have required consumers to change their passwords due to cyber-attack. In eBay's case, they issued a press release stating that customer name, encrypted password, date of birth, email address and phone number were all compromised, but it did not believe that financial information was affected: eBay Inc., 'Ebay Inc. to ask eBay users to change passwords' (21 May 2014 accessed 21 May 2014) <http://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/> Consumers are also well aware of infamous hacking incidents such as the Heartland Payment Systems breach when 134 million credit cards were stolen in 2008. See for more examples, not necessarily cloud-related: Amerding, above n 20.

[156] The International Working Group on Cloud Computing Resiliency, Downtime statistics of current cloud solutions 2007–2012: http://iwgcr.org/wp-content/uploads/2012/06/IWGCR-Paris.Ranking-002-en.pdf cited in Mark Vincent and Katrina Crooks, 'Cloud Computing in 2013 - What legal commitments can you expect from your provider?' (18 Feb 2013 accessed 11 July 2014) http://www.shelstonip.com/case_study.asp?cid=13.

[157] Websitehostreview.com, 'The Dark Side of the Cloud' *Infographic* (Mar 20th, 2014 accessed 16 June 2014) http://i2.wp.com/www.thecloudinfographic.com/wp-content/uploads/2014/03/dark-side-of-the-cloud-infographic.jpg.

[158] This occurred (in different ways) in both the Dropbox and Apple iCloud cases.

[159] InfoWorld, 'Popular cloud sync app raises security fears' *Tech Watch (8 Nov 2011 accessed 30 July 2014)* <http://www.infoworld.com/print/157776>.

[160] Alan Pawlak, head of client services, Aetna cited by Stacy Collett, 'How to recover after a cloud computing misstep' *Computerworld* (July 1, 2014 accessed 9 July 2014) <http://www.computerworld.com/s/article/9248619/How_to_recover_after_a_cloud_computing_misstep>.

[161] Roy Morgan Research reports that in the year to March 2013, online spending increased 11.9% to $24.9 billion in Australia. ABS data for that period shows that total retail sales only grew to 3.4% to $258.4 billion, and Roy Morgan estimate that 9% of that is now spent online (c/f 5% in previous surveys). It is also the first time that this survey (of over 50,000 individuals) has shown that a majority of Australians used purchased online in any survey period: Roy Morgan Research, 'State of the Nation's $24 billion online retail trade: Internet shopping becomes the new Australian norm' (4 June 2014 accessed 17 July 2014) <http://www.roymorgan.com/~/media/Files/Findings%20PDF/2013/June/4946%20%20State%20of%20the%20Nation%2014%20%20Online%20Shopping%20March%202013.pdf>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

of cloud services,[162] from the provision of online software to storage to cloud platforms. It is both ubiquitous and legally problematic, particularly when it comes to consumer contracting, much of which is conducted in a non-negotiable standard form context and arguably, often occurs with little regard for legal conceptual issues such as capacity, consent, fairness and so on. These issued are exacerbated by an often manipulated online marketing context.[163] It seems likely that conceptual and practical contracting issues will increase in prominence over the next few years as cloud computing grows and both the ACCC and consumers focus more closely upon cloud computing legal rights and responsibilities.

3.3.1. *Consumer trust in industry compliance*

Gartner reports three factors as to business cloud contracting: buyers are increasing but "… are being asked to trust the providers, without any legal motivation on the part of the service provider,"[164] cloud terms and conditions are maturing, but contracts still require heavy negotiation by "… IT procurement professionals to avoid unacceptable costs and risk; and thirdly, changing standard cloud contract terms and conditions remains a challenge."[165] If this is business experience, then consumer experience is even more challenging, particularly given the almost universal prevalence of standard form contracts.[166] Common high risk areas for consumers in this regard are privacy, data location and (international) regulatory access; service availability; ability to transition services; unilateral variation without notice and termination rights; choice of law and jurisdiction clauses and security including breach notification. The question is whether consumer laws are impacting upon these terms and contracts generally, in such a way as to make them fair to consumers? As the discussion on unfair contract terms supported by Annexure Three suggests (supra), the answer would appear to be 'not yet'. [Annexure Three is available online as "supplementary material" on ScienceDirect].

This is significant given that unfair terms regimes have now been in place in Europe and Australia for a number of years – yet many international cloud providers are clearly not responding as the law requires. As such, it seems that consumers cannot reply upon cloud industry members to voluntarily regulate their own contracting behaviour, even under the shadow of the law.

3.3.2. *Words & meanings*

Research evidences that consumers do not read online terms and conditions, do not understand them fully and that many of the terms are unfair and potentially unconscionable.[167] A 2009 US study showed only one or two of every 1000 purchasers accessed online terms and conditions and those that did only read a small proportion of the text. Consumer Affairs Victoria research shows a quarter of consumers fail to read contracts, and another 21% only gave them "cursory consideration".[168] From the perspective of potential unfairness and even unconscionability, it is useful to consider why this is the case.

Apple iTunes terms and conditions are 19,972 words long, almost 2000 words longer than Shakespeare's *Macbeth*.[169] IDG report that the median terms and conditions word count for the top 75 US websites is 2,514,[170] with facebook at 11,195, LinkedIn at 7,294, twitter on 3486 and Google+ on 1691.[171] Length itself is inherently off-putting to consumers, and

[162] The Organisation for Economic Co-operation and Development (OECD) define e-commerce as the sale of goods and/or services "which are ordered via the Internet or any other computer-mediated network … regardless of whether the payment and/or the ultimate delivery of the goods and/or services is conducted online or offline". The ABS conclude therefore, that "all retail trade activity where the commitment to purchase is made online may be considered to be online retail trade activity, irrespective of the method of payment and/or delivery used": Australian Bureau of Statistics, '8501.0.55.007 - Information Paper: Measurement of Online Retail Trade in Macroeconomic Statistics, 2013' (19/08/2013 accessed 17 July 2014) <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8501.0.55.007Main%20Features12013?opendocument&tabname=Summary&prodno=8501.0.55.007&issue=2013&num=&view=>.

[163] While it seems odd to assert a private online transaction can be pressured, marketers employ various tactics such as dark patterns, drip pricing and the like, which may manipulate consumers in a contracting context.

[164] Gartner, Gartner 'Predicts 2013: Cloud and Services Security' (28 November 2012 accessed 18 June 2014) <https://www.gartner.com/doc/2254916?ref=SiteSearch&sthkw=predicts%202014&fnl=search>.

[165] Gartner, 'Cloud Sourcing: Lessons Learned from the Early Adopters' (21 May 2012 accessed 18 June 2014) <https://www.gartner.com/doc/2022215?ref=ddisp>.

[166] For a discussion of 'free' services and recent German case law see Part 6.

[167] Consumer Affairs Victoria, 'Unfair Contract terms in Victoria: Research into their extent, Nature, Cost and Implications' *Research Paper No. 12* (October 2007 accessed 5 Aug 2014) [15] <http://www.consumer.vic.gov.au/resources-and-education/research>.

[168] CAANZ, above n 88.

[169] Swinhoe, above n 30. *Macbeth* is 18,110 words in length.

[170] A 2012 privacy policy study of the 75 top US websites suggests that the median length of their privacy statement is 2514 words and would take a consumer 10 min to read. Given terms and conditions are usually equivalent to or longer than the privacy statements, this extrapolates to at least 20 min to read the contractual terms and conditions: Aleecia M. McDonald and Lorrie Faith Cranor 'The Cost of Reading Privacy Policies' *I/S: A Journal of Law and Policy for the Information Society* (2008 accessed 29 July 2014) http://www.is-journal.org/ <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf> The authors calculated the average privacy policy read time using the 75 most popular websites and an assumed 250 word per minute average reading rate. Using the 10 min average reading time per policy, then known numbers of Americans online and average website use (using Nielsen/Net Ratings and Pew data) plus time valued at double wages for work and 25% average hourly salary for leisure, the survey found that the national opportunity cost in time to read policies was $781 billion. They conclude that adding in comparison time to allow informed decision-making plus individual privacy "value" to the individual, meant that "targeted online advertising may have negative social utility". See also Alexis C Madrigal., 'Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days' *The Atlantic* (1 Mar 2012 accessed 27 July 2014) <http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[171] Swinhoe, above n 30. Others include Reddit on 5706 and MySpace on 5486.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

may even constitute a factor in finding a contract term to be unfair according to recent UK authority.[172] The point is borne out when an online gaming store facetiously inserted an "immortal soul clause" in their website terms and conditions. In one day, 7500 consumers granted *Gamestation* a non-transferable, eternal option to claim their "immortal soul"[173] upon notice served "in 6 (six) foot high letters of fire" and without liability for loss or damage thereby caused.[174] Only 12% of consumers selected "click here to nullify your soul transfer";[175] the rest (presumably) did not read the terms and conditions. IDG also report that 93% of users do not read website terms and conditions,[176] of which 43% complain that they are too "boring", cannot be understood and 58% said that they would rather read their utility bill.[177] The gist is that consumers find that online terms and conditions are too long, contain legalese or wordings which consumers cannot understand, and are therefore not accessible to the average person. In other words, they lack *transparency*.

These factors are precisely the sort of factors which might form the basis for an action under the unfair contracts provisions in section 23 of the ACL and possibly, in unconscionability (both discussed below). Aside from these serious fairness issues, one survey suggests that consumers are suffering adverse outcomes as a result: one in five (21%) have ticked a consent box without realising all relevant contract terms, which include, for example, 10% being locked into a longer term contract than expected and 5% losing money due to non-cancellation clauses.[178]

3.3.3. *Enforceability/validity: general contracting issues*

It is now well established that electronic contracts – such as those pertaining to the free use or commercial purchase of cloud products – are (usually) legally enforceable in Australia and many other countries around the world.[179] The *Electronic Transactions Act 1999* (Cth) paved the way for uniform state legislation across Australia.[180]The legal issue is the contractual requirement for consent. If a buyer does not really read the contents of a contract – such as is required to use a cloud service – are they bound by its terms? The general contractual answer is yes – provided that either the terms are so obvious that a consumer should have noticed them pre-contract formation or reasonable steps are taken to ensure a buyer's attention is drawn to the terms and conditions, and the buyer has clicked through saying 'yes'. In this situation, generally, consent is presumed to be valid.[181] Of course, this applies unless ACL issues of unfair terms, unconscionability, misleading or deceptive conduct or false representations apply, which are considered in the next section.

4. Consumer laws & some 'cloudy' cases

> *…cloud computing is not a technological revolution that requires separate, cloud-specific rules…*[182]

Cloud computing is subject to four principal forms of national regulation in Australia: the *Australian Consumer Law*, general contract law governing contractual relations between provider and user (and intermediaries); the *Privacy Act* and ASIC's ePayments Code (ePC).[183] The complexity and scope of privacy law issues in an online/cloud context warrants a separate paper and the ePC is discussed only briefly under part 4.2 below. This paper therefore focusses on the former two.[184]

[172] *Spreadex Ltd v Cochrane*[2012] EWHC 1290.

[173] Fox News, '7500 Online Shoppers Unknowingly Sold Their Souls ' (15 April 2010 accessed 24 June 2014) <http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/>.

[174] "By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant us a non-transferable option to claim, for now and forever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorized minions." See Catharine Smith '7500 Online Shoppers Accidentally Sold Their Souls to Gamestation' *Huffington Post* (25 May 2011 accessed 21 June 2014) <http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html>.

[175] These consumers received a 5 GBP coupon for noticing the link. The clause went on: "we reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction."

[176] Swinhoe: above n 30.

[177] Skandia, 'Skandia Takes the Terminal out of Terms and Conditions' *Press Release* (16 May 2014 accessed 29 July 2014) <http://www2.skandia.co.uk/Media-Centre/2011-press-releases/May-2011/SKANDIA-TAKES-THE-TERMINAL-OUT-OF-TERMS-AND-CONDITIONS/#sthash.mR0PwsBL.dpuf>.

[178] Ibid.

[179] Jay Forder & Dan Svantesson, *Internet & Ecommerce Law* (Oxford University Press, 2010): above n. 81: 34–35. Note the United Nations Commission on Electronic Trade Law (UNICTRAL) *Model Law on Electronic Commerce*, GA Resolution 51/162, GAOR 51st sess, 85th plen mtg, UN Doc A/Res/51/162 (1996) which has formed the basis for legislation in over 50 countries and states: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html See note 180 below for the relevant Australian legislation.

[180] Other relevant legislation is the *Electronic Transactions (Queensland) Act 2001 (Qld), Electronic Transactions (Victoria) Act 2000 (Vic), Electronic Transactions Act 2000 (NSW), Electronic Transactions Act 2000 (SA), Electronic Transactions Act 2000 (Tas), Electronic Transactions Act 2001 (ACT) and Electronic Transactions (Northern Territory) Act 2000 (NT) and Electronic Transactions Act 2003 (WA).*

[181] See the discussion in Forder, above n 179: chapter 4.

[182] Stakeholder (unnamed) cited in Aust Govt Regulatory Stocktake, above n 36: 9.

[183] The Code "… complements other regulatory requirements, including financial services and consumer credit licensing, advice, training and disclosure obligations under the *Corporations Act 2001* and the *National Consumer Credit Protection Act 2009*.': ASIC, ePayments Code (1 July 2012 accessed 15 July 2014) <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/ePayments-Code-as-amended-from-1-July-2012.pdf/$file/ePayments-Code-as-amended-from-1-July-2012.pdf>.

[184] The author proposes to address the other two issues in a companion paper.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

4.1. *Consumer laws: an overview*[185]

> *You are entitled to expect every business you deal with to honour its obligations under the Australian Consumer Law…*[186]

The Australian Competition and Consumer Commission (ACCC) claims to be closely "watching" the cloud industry, but has done little work on consumer issues arising from the cloud, including computing contracts.[187] The ACL establishes an extensive national consumer protection regime effective on and from 1 January 2011.[188] The principal provisions relevant to consumer cloud issues are prohibitions upon misleading and deceptive conduct or false representations, unconscionable conduct, statutory unfair contract terms and consumer guarantees. Remedies available to both the regulator[189] and successful plaintiffs,[190] are extensive. It is therefore very likely that the ACCC will turn its attention to the cloud computing industry in the near future.

4.1.1. *Threshold issues*

The ACL provisions contain various threshold matters which must be satisfied before the ACL can apply: firstly, the definitions 'person' and 'in trade or commerce' and secondly, issues as to jurisdiction and enforcement. These warrant a brief discussion.

Person: Cloud providers are usually corporations which are included under the ACL as 'persons' and are usually regarded as 'carrying on business within Australia', either through doing business with an Australian consumer or through physical presence (for example, by representative offices or data centres) and therefore their conduct is captured under these provisions.[191]

'in trade or commerce': This phrase means trade or commerce within Australia or between Australia and any place(s) outside, and includes 'any business or professional activity (whether or not carried on for profit)'.[192]

Governing Law & Jurisdiction: There is room for legal argument disputing jurisdiction where the provider is overseas-based and the contract prescribes an overseas choice of law to suit the provider, as is commonly the case. For example, Apple's iCloud terms[193] prescribe the laws of California as the governing law (excluding its conflicts of law provisions) and only allow the laws of a consumer's usual place of residence to apply where mandated, such as in the EU.[194] Section 67 of the ACL provides that if the 'proper law' is Australian, it shall apply regardless of any contrary contractual term; in turn, this requires a court to consider the facts of the case, including the parties' location, where the services are provided, where the contract was formed, the location of the equipment, as well as the contractual terms. As such, there is no certainty that proceedings can be commenced under Australian law in Australia which is obviously the better forum for an Australian consumer for cost and convenience reasons. Note the comments in Annexure Three [Available online as "supplementary material" on ScienceDirect] as to jurisdiction clauses which uniformly favour the cloud provider – and the possibility that these might form the basis for an unfair contract term argument.

[185] This section considers a basic overview (rather than summary) of the potentially relevant ACL provisions; it does not purport to summarise the law but rather seeks to highlight its application to potential cloud computing issues.

[186] Michael Schaper, 'Speech to Council of Small Business of Australia National Small Business Summit, Sydney' *Australian Competition and Consumer Commission* (27 July 2011 accessed 17 July 2014) [1] <http://www.accc.gov.au/system/files/SPEECH%20-%20M%20Schaper%20-%20COSBOA%20-%2027%20July%202011%20FOR%20WEB.pdf>.

[187] "The ACCC will be closely watching key areas of interest as Cloud computing becomes more widespread": Peter Kell, 'Implications of cloud computing for consumers' *Presentation to the Global Access Partners Workshop on Cloud Computing* in Global Access Partners Pty Ltd, 'GAP Workshop on Cloud computing' Report (24 June 2011 accessed 11 July 2014) <http://www.globalaccesspartners.org/GAP-Workshop-on-Cloud-Computing-Report.pdf> The first case involving consumer guarantees and an online gaming cloud service, is *Australian Competition and Consumer Commission v Valve Corporation* [2014] FCA 1018 – which is to be heard in mid-2015.

[188] Note that the unfair contract terms provisions of the ACL commenced earlier – they are effective 1 July 2010.

[189] In addition to the remedies itemised in fn below, ACL Part 5-1 contains non-court imposed enforcement powers including powers to accept undertakings, substantiation notices and the power to issue public warning notices. Section 134A CCA enables the ACCC to issue infringement notices in lieu of civil penalty proceedings as well.

[190] ACL Ch 5 powers include injunctive relief, pecuniary penalties and compensation orders.

[191] As a Commonwealth law, the ACL applies to any trading or financial corporation formed within Australia or incorporated within a territory of Australia, or a foreign corporation (or a holding company of any of these): *Competition and Consumer Act 2010 (Cth)* sections 4 and 13(1). It applies to individuals as an "application law of states and territories": Stocktake, above n 36.

[192] ACL section 2.

[193] Apple Inc., 'iCloud Terms and Conditions' (accessed 12 July 2014) http://www.apple.com/legal/internet-services/icloud/ww/including Australia (18 Sept 2013) <http://www.apple.com/legal/internet-services/icloud/en/terms.html> Note also that the ACCC instituted *Australian Competition and Consumer Commission v Valve Corporation* [2014] FCA 1018 in late 2014. The case is presently awaiting court-ordered mediation, but may require the Federal Court to consider the proper law of an online contract specifying US law, as between Valve Corporation and Australian consumers purchasing online access to video games. Valve argues that the consumer guarantees do not apply to a supply under that contract under ACL section 67: see the discussion in Patrick Gunning, 'All steamed up about consumer guarantees', *King & Wood Mallesons*, 9 Sept 2014 accessed 4 Nov 2014 <http://www.incompetition.com.au/2014/09/steamed/>; Patrick Gunning, 'Consumer guarantees-an update on the steam case' *King &Wood Mallesons* (31 Oct 2014, accessed 4 Nov 2014) <http://www.incompetition.com.au/2014/10/consumer-guarantees-update-steam-case/>.

[194] To the extent that the protections under the selected law do not derogate from the protections of the laws of their home jurisdiction, consumers are permitted to select the applicable law of a contract: Council Regulation 593/2008 on the Law Applicable to Contractual Obligations (Rome I) cited in James J. Healy, 'Consumer Protection Choice Of Law: European Lessons For The United States' *Duke Journal of Comparative and International Law* 19: 535–558.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

Aside from all of these issues above, there may be practical enforcement issues if the cloud provider is based outside Australia: for example, the cost to the consumer of pursuing proceedings or enforcing any judgment obtained – particularly against a well-resourced, multi-national corporation – may be prohibitive.

4.1.2. *Parts 2-1 and 3-1 misleading conduct and representations*

> *Online competition and consumer issues are a priority for the ACCC… [online trader] obligations are the same as traditional retailers' and must not mislead customers or other businesses…*[195]

Cloud vendors are retailers of a product which is commonly sold and supplied online. Section 18 of the *ACL*[196] provides that a 'person shall not in trade or commerce engage in conduct which is misleading or deceptive or which is likely to mislead or deceive'. To this norm of conduct is added section 29, which deals extensively with false representations made in business in connection with the supply, acquisition (or possible supply or acquisition) or promotion of goods or services, and prohibits false or misleading representations, inter alia, (a) that goods are of a particular standard, quality, value, grade, composition, style or model … (b) or that services are of a particular standard, quality, value or grade; or (g) have a sponsorship, approval, performance characteristics, accessories, uses or benefits; or (i) as to price; or (l) the need for any goods or services; or (m) concerning existence, exclusion or effect of any condition, warranty, guarantee, right or remedy; or (n) concerning a requirement to pay for a contractual right (including statutory guarantee or other legal right).

These provisions are commonly used with respect to marketing, advertising or other representations as to supplier, product or service performance and so clearly have application to a cloud consumer context. A consumer who purchases a cloud service which for example, fails to meet technical, service or security levels promised or which fails to contain features or uses promised, or which despite security promises, causes damage or loss to consumer data, or which fails to comply with contractual warranty or statutory guarantee obligations, could potentially take an action alleging breach of sections 18 and 29. The remedies for breach are comprehensive, including fines[197] of up to $1.1 million for corporations and $220,000 for individuals.

4.1.3. *Part 2-2 unconscionable conduct*

The ACL prohibits unconscionable conduct in the supply of goods and services under section 21.[198] It is actionable by individual consumers and SMEs[199] but most case law arises within an interpersonal context, rather than online. Statutory unconscionability is not defined[200] but is determined based upon sections 21[201] and the non-exclusive criteria in section 22. This latter section prescribes a long list of non-exclusive factors the court must consider: these include the relative bargaining strengths of the parties;[202] whether the supplier conduct required the customer to comply with conditions not reasonably necessary to protect the legitimate interests of the supplier;[203] whether the customer was able to understand the documents;[204] any undue influence or pressure or unfair tactics on the customer,[205] the amount and circumstances under which the customer could have obtained equivalent or identical goods or services;[206] the extent the supplier's conduct was consistent with its conduct to others in similar transactions;[207] the requirements of any industry code(s);[208] the extent to which the supplier fails to disclose any intended conduct which might affect the customer's interests or any foreseeable risks not apparent to the customer;[209] and the extent to which the supplier acted in good faith.[210] In addition, section 22(1)(j) specifically refers to the contract and includes: the extent to which the supplier was prepared to negotiate the contract, the contract terms and conditions, including any

[195] Rod Simms, ACCC Chair quoted in Michael Bailey, 'Scoopon hit with $1 million fine and 'community service' *BRW* (17 December 2013 accessed 9 April 2014) <http://www.brw.com.au/p/business/scoopon_hit_with_million_fine_and_Uatxc0xk9W7H5xJUy1lEWL>.

[196] The ACL is found in the CCA Schedule 2. Note that it is a national law such that state fair trading and related legislation mirror the national provisions. As such, they are not dealt with separately here.

[197] CCA uses the term 'pecuniary penalties' to avoid the criminal standard of proof.

[198] ACL section 20 prohibits unconscionable conduct "within the meaning of the unwritten law from time to time" which applies to conduct which does not involve the supply or acquisition of goods or services, hence is less likely to be of relevance in a cloud computing context. Note that equitable unconscionability is interpreted by the courts to mean where an innocent party acts under a 'special disadvantage', the other party has actual or constructive knowledge of that disadvantage and unfairly or unconscientiously exploits that disadvantage. In these circumstances, the courts have traditionally placed the onus upon the stronger party to show that the transaction was fair, just and reasonable. 'Special disadvantage means a serious disadvantage beyond just an inferior bargaining position or commercial vulnerability and extends beyond mere inequality of bargaining power, such as that which exists between a consumer/SME and an entity such as Microsoft. See *Blomley v Ryan* (1956) 99 CLR 362 & *Commercial Bank of Australia v Amadio* (1983) 151 CLR 447.

[199] See s 21(1) It applies to businesses other than a listed public company.

[200] Section 20(2) provides that equitable unconscionability does not apply to situations under which section 21 as to unconscionable conduct in connection with the supply or acquisition of goods and services, applies.

[201] The ACL provides that the court *may* consider the contract terms, the manner in which and extent to which it was carried out and is "not limited" to considering the contract formation circumstances.

[202] ACL s 22(1) (a).

[203] ACL s 22(1) (b).

[204] ACL s 22(1) (c).

[205] ACL s 22(1) (d).

[206] ACL s 22(1) (e).

[207] ACL s 22(1) (f).

[208] This includes any code the customer acted on reasonable belief that the supplier would comply with it: s 22(1)h).

[209] ACL s 22(1) (i).

[210] ACL s 22(1) (l).

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

unilateral right of variation,[211] the party's conduct in complying with its terms and any post-contractual conduct of either party.

There is no authority in Australia applying unconscionability to a cloud computing context,[212] but an argument might well be constructed whereby multiple contractual factors such as clauses exploiting an obvious inequality of bargaining power,[213] unilateral cloud provider contract variation rights, non-negotiability, terms not reasonably necessary to protect the provider's legitimate interests – and the like - might be pleaded together in order to establish that a cloud provider has acted unconscionably towards a consumer. This might especially be the case in circumstances where the cloud provider takes advantage of consumer technical ignorance or fails to explain risks not foreseeable to an average consumer[214] or where the consumer is exploited as a result of a personal vulnerability of which the cloud provider is (somehow) aware. As the section applies to conduct both before and after the contract formation, e-commerce purchases via websites or subscription services are also encompassed[215] – so unconscionable sales processes such as dark patterns, drip pricing or perhaps even, long and legalistic terms and conditions online[216] (especially where access to legal advice is not readily available) might also be actionable either alone or in conjunction with unconscionable marketing, contractual terms or conduct, in the right circumstances. Note however that some US authority suggests that the existence of competition in the cloud market and alternative offerings of cloud services may mitigate against a finding of unconscionability.[217] In other words, the consumer could go elsewhere.

The ACL remedies are extensive.[218] It is probable that any action in unconscionability would be pleaded in conjunction with claims under the unfair terms regime. These provisions are considered next.

4.1.4. *Part 2-3 unfair contract terms*

The unfair contract term provisions render void unfair terms in a 'standard form'[219] 'consumer contract'[220] made, renewed or varied after 1 July 2010.[221] Give the ICT sector tends to use arguably provider-biased standard form contracts, and consumers are generally unable to negotiate those terms,[222] these provisions have become particularly relevant in both Australia and the EU.

A term is unfair if three criteria apply: firstly, it would cause a significant imbalance in the parties' rights and obligations arising under the contract, secondly, it is (presumed)[223] not to be reasonably necessary to protect the legitimate interests of the advantaged party; and thirdly, it

[211] ACL s 22(1) (k).

[212] There is an authority pertaining to online advertising: *ACCC v Zanok Technologies Pty Ltd* [2009] FCA 1124; *Caspi v Microsoft Network* LLC 323 N.J. Super 118 (NJ Super Add Div 1999).

[213] The High Court has stated that inequality of bargaining power alone cannot constitute equitable unconscionability – this is likely to be persuasive as to section 21 statutory unconscionability: *ACCC v Berbatis* (2003) 214 CLR 51.

[214] An analogous circumstance might be *ACCC v Keshow* [2005] FCA 558 involving sales of educational materials to indigenous people who it seems, did not understand what was being sold to them or how it would be billed.

[215] Note that the ACL apply to these which will include misleading processes for ecommerce purchases. Note the non-binding ecommerce Guidelines recommend appropriate practices for ecommerce including (inter alia) that providers must ensure practices which allow consumers to review, accept or reject contract terms and conditions, identify and correct any order errors and to confirm or reject the offer. See Department of Treasury, 'The Australian Guidelines for Electronic Commerce' (2006 accessed 4 Aug 2014) <http://archive.treasury.gov.au/contentitem.asp?ContentID=1083>.

[216] Note however, authority under a previous incarnation of the ACL held that unconscionability requires some circumstances beyond mere contractual terms that would render reliance upon them unreasonable, unfair, wrong or immoral: *Hurley v McDonald's Australia Ltd* (2000) ATPR 41-741 [31] as discussed in Dan Jerker Svantesson, 'Unconscionability' in Consumer Ecommerce' *Commercial Law Quarterly: The Journal of the Commercial Law Association of Australia* 25:1 (Mar/May 2011 accessed 23 May 2014) [11] <http://search.informit.com.au.ezproxy.bond.edu.au/documentSummary; dn=043279687656685;res=IELHSS> <ISSN: 0819-4262> It is possible that this case would be distinguished given the context, which was a franchise relationship – the earlier case of *George T Collings (Aust) Pty Ltd v H F Stevenson (Aust) Pty Ltd* (1991) ATPR 41-104 [52,622 – 3] found that an onerous standard form contract term could not be relied upon as it was unconscionable.

[217] *Caspi v Microsoft Network* LLC 323 N.J. Super 118 (NJ Super Add Div 1999).

[218] Depending upon who institutes the action (a 'customer' or the ACCC), remedies include undertakings (s. 218); substantiation notices (s. 219); public warning notices (s. 223); pecuniary penalties (s. 224); injunctions (s. 232); damages (s. 236 subject to CCA s. 137B); compensation or other orders (s. 237); non-punitive orders (s. 246); adverse publicity orders (s. 247); disqualification orders (s. 248) and infringement notices (s. 134A CCA).

[219] ACL section 27 imposes a presumption that the contract is standard form, unless another party in the proceeding proves otherwise – by reference to ss(2) which lists (a) whether one party has most of the bargaining power; (b) whether the contract was pre-prepared by one party; (c) whether one party was required to "accept or reject" those terms; (d0 whether there was effective opportunity to negotiate the terms; whether the terms take into account the specific characteristics of another party; and (f) any other matter prescribed in the regulations.

[220] A consumer contract, as discussed above in part 2, means a contract for the supply of goods or services to an individual who subjectively acquires them for personal, domestic or household use or consumption. Part 2-3 does not apply to a contract to supply goods or services for business use between businesses.

[221] Note these provisions came in six months earlier than other ACL provisions. With respect to the Cth, contracts entered into or varied after 1 Jul 20120 are covered, those varied or renewed apply only to the extent of the renewal or variation: *Trade Practices Amendment (Australian Consumer Law) Act (No 2)* Schedule 7, section 8(2).

[222] Most cloud contracts are presented on a take-it-or-leave-it basis which reflects administrative convenience, as well as inequality of bargaining power. The consumer who wants iCloud is not in a position to call Apple and seek to amend terms. In contrast, the City of Los Angeles achieved some significant concessions: City of Los Angeles, Professional Services Contract between the City of Los Angeles and Computer Science Corp. for the *Saas* E-Mail and Collaboration Solution (SECS) (2009), available at <https://sites.google.com/a/lageecs.lacity.org/la-geecs-blog/home/faqs-1/C-116359_c_11-20-09.pdf?attredirects=0&d=1>.

[223] ACL section 24(4) imposes a presumption against the party advantaged by the term.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

would cause detriment (financial or other) to a party were it applicable or relied upon. The court may take account of factors it thinks relevant and must take into account both transparency[224] and the whole contract.[225] Section 25 lists fourteen 'examples', which are extracted in Annexure Three [See supplementary material online], together with an appraisal of four randomly-selected cloud contracts. This simple study suggests that a term may be unfair where cloud providers have powers or rights not available to the consumer, such as unilaterally varying the nature, size, speed, security levels or other important features of cloud services and reveals that while cloud contracts may have improved, there are still questionable terms as to fairness in most of the large provider's contracts. As Annexure Three shows, terms such as unilateral variation rights and service changes – and even cessation of service – are included. That none of the four providers randomly selected had a contract free of potentially unfair terms (in the author's opinion) suggests that these form a common component of cloud computing contracts[226] – which is why it is suggested that as the cloud consumer market matures, consumers may avail themselves of ACL provisions to either avoid unfair terms or indeed, entire contracts if they are rendered inoperable by severance. This is in addition to any complementary action pleaded under sections 18 or 29 as discussed above.

This prospect has eventuated recently in Germany.[227] In *In re Google, Inc.*,[228] the Berlin District Court held that 25 terms in Google's online Terms of Use and its Privacy Statement, are unenforceable.[229] The case is significant in several respects; firstly, the court found that the terms create legally enforceable contracts whereas Google had (ironically) argued that as the services are 'free', there is no valid contract. The court very practically found that the requirement to consent to terms upon registration meant that there is an exchange for value, as Google obtains the registrant's commercially-valuable personal data for marketing purposes.[230] It is the author's view that the same approach should be taken in Australia with respect to whether or not such services are provided "in trade or commerce" under the ACL[231] – as the obtaining and use of such data is within the trading activities of free service providers. There seems little doubt that cloud providers contractual dealings with consumers bear a commercial character[232] where selling paid cloud services, and based upon the German case, the same applies given the 'business activities' of obtaining consumer information for use or with the intention of advertising or creating saleable data sets as to such people[233] via their free service offerings.[234] Secondly, the Google case is significant in indicating the types of terms which may be 'unfair': unilateral termination, the monitoring of content for policy compliance, unilateral alteration of service; variation to terms of use without consent and the (mutual) limitation for liability as to statutory product liabilities. The final interesting aspect was that as Google's privacy consents[235] did not meet German privacy disclosure requirements, ticking the consent box did not constitute valid consent.[236] The case is potentially, very significant were elements of its findings to be adopted in Australia.

[224] Section 24(3) defines transparency as a term expressed in reasonably plain language, legible and presented clearly readily available to any party affected by the term: ACL section 24(3).

[225] ACL section 24(2). Note that section 23 does not apply to any term which defines the subject matter of the contract (that is, consideration payable disclosed when the contract is entered into but excludes any consideration contingent upon the happening or non-happening of any particular event: ACL section 26(2). or sets the upfront price payable under it; or is a term expressly required by law: ACL section 26.

[226] The author subsequently searched out an example of 'good' cloud contracting and at least in terms of transparency, concludes that Dropbox has adapted a consumer-friendly approach: DropBox 'Terms of Service' (20 Feb 2014 effective 24 March 2014 accessed 19 June 2014) https://www.dropbox.com/terms.

[227] Subject to appeal in the Google case: below n 231.

[228] *In re Google, Inc.*, LG Berlin, No. 15 O 402/12, 11/19/13. There is no English translation of this case available on the internet. As such this discussion is reliant upon secondary sources.

[229] Note the German unfair contract terms legislation specifies that terms which conflict with the "main elements of German law and unfairly disadvantage consumers" are invalid. Google will appeal the application of this clause, arguing that the German *Federal Data Protection Act* and the *Telemedia Act* do not apply as they are limited to organizations established in Germany or which use equipment in Germany.

[230] Retzer, Karin 'German Court Finds 25 Provisions in Google's Online Terms of Use and Privacy Policy to Be Unenforceable' *Morrison & Foerster LLP* (20 Dec 2013 accessed 10 Aug 2014) <https://www.jdsupra.com/legalnews/german-court-finds-25-provisions-in-goog-45359/>.

[231] The ACL definition includes 'any business or professional activity whether or not carried on for profit": ACL s 2.

[232] *Hearn v Rourke* [2003] FCAFC 78 per Dowsett, J the focus must be on the conduct in question – which on the facts of In re Google, above n 230 included the terms enabling the commercial use of the consumer information.

[233] A similar though not analogous fact situation is solicitation by mail for subscribers for UK books etc, which conduct was held to be "in trade or commerce": *Swan v Downes* (1978) 34 FLR 36 c/f *E v Australia Red Cross Society* (1991) 27 FCR 310 where the provision of free blood was held to be not" in trade or commerce".

[234] An extension of the argument might be to suggest that promoting such services as "free" breaches ACL section 18 insofar as whilst there is no apparent cost, the consumer is supplying data which has commercial value to the cloud provider. This would be an unlikely extension to the law (which tends to focus directly upon the representation with respect to whether a consumer must pay or lose money directly in some way) but would more realistically reflect the exchange between the parties – and seems open on the reasoning of the German case.

[235] Spain and Germany are threatening financial sanctions because the privacy terms fail to comply with their privacy laws: Loeb Essers, 'Berlin court rules Google privacy policy violates data protection law' (20 Nov 2013 accessed 10 Aug 2014) <http://www.cio.com/article/2380759/legal/berlin-court-rules-google-privacy-policy-violates-data-protection-law.html>.

[236] Ibid.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

The first Australian unfair terms case is ACCC *v Bytecard*[237] which resulted in an adverse costs order and a consent declaration that four contract terms in an ISP contract were invalid. The impugned terms were one enabling unilateral variation of the amount payable without prior notice,[238] a broad, non-reciprocal indemnity[239] and a termination clause whereby the supplier could terminate at will, but the consumer was only allowed to do so subject to conditions.[240] Given European developments in this area, it seems likely that the ACCC could consider far greater enforcement action in the cloud industry in near future.[241]

4.1.5. *Part 3-2 consumer guarantees*

Every contract for the supply of goods or services in trade or commerce to a consumer contains consumer guarantees which cannot be excluded, restricted or modified by contract.[242] There are nine guarantees as to 'goods' and three as to 'services', which makes the distinction important to consumers' rights.

If a cloud service is held to provide 'software' and thereby supplies a 'good', there are various applicable guarantees of title,[243] undisturbed possession,[244] no undisclosed securities,[245] acceptable quality,[246] fitness for disclosed purpose,[247] correspondence with description or sample,[248] availability of repairs and spare parts,[249] and as to mandatory compliance with express warranties.[250] From a cloud consumer perspective, the most important is that the goods are of *acceptable quality* – as this requires the software to be fit for all reasonable purposes goods of the kind are commonly supplied, acceptable in appearance, free from defects, safe and durable as a reasonable consumer, fully acquainted with the state of the goods and any hidden defects in them, would regard as 'acceptable'. This test is balanced against factors such as the nature and price of the goods, representations of the supplier and any other relevant circumstances. It is clear that a consumer might mount an action for software supplied which (for example) fails or which suffers outages, is unreasonably susceptible to attack or viruses, or which fails to conform with description or advertised features or performance levels; whether these matters are within the expectation of a reasonable software acquirer is a matter for the court to decide – and there is potentially an argument for providers to assert a lower consumer expectation standard generally across IT having regard to the nature of the industry and nature of the products supplied.

Where a cloud service is a '*service*' (which seems more apposite), then there is a guarantee (inter alia)[251] that the supplier will render those services with due care and skill,[252] and that the services *and any product resulting from them*, will be reasonably fit for that purpose.[253] This guarantee requires that the consumer makes known "expressly or by implication" the purpose. Likewise, a consumer may make known expressly or by implication a "result that the consumer wishes to achieve", and then there is a guarantee that the services and product will be of "such nature, and quality, state or condition, that they might reasonably

[237] Simon Uthmeyer, Fleur Gibbons, Geoff Taperell and Leanne Hanna 'ACCC obtains its first unfair contract terms declaration: *ACCC v Bytecard Pty. Limited*' DLA Phillips Fox (4 Aug 2013 accessed 7 Aug 2014) <http://www.mondaq.com/australia/x/255956/Consumer+Trading+Unfair+Trading/ACCC+obtains+its+first+unfair+contract+terms+declaration+ACCC+v+Bytecard+Pty+Limited>.

[238] Section 1.7: NetSpeed reserves the right to change prices or services at any time without prior notice to customers or the public, except when the service is an Australian Broadband Guarantee Service. Price changes will not be retroactive for existing prepaid customers. It is the User's responsibility to check this online.

[239] Section 4.1: The User agrees to indemnify and hold NetSpeed, its affiliates, its licensers, its contractors or their respective employees harmless against any and all liability, loss claim, judgment or damage. This indemnity includes, but is not limited to an indemnity against all actions, claims and demands (including the cost of defending or settling any actions, claim or demand) which may be instituted against us, as well as all expenses, penalties or fines (including those imposed by any regulatory body or under statute).

[240] Section 4.2: The User agrees to indemnify NetSpeed for any expenses including, but not limited to: 1. attorney's fees and cost of litigation, 2. its licensers, 3. its contractors or their respective employees as the result of any and all use of User's account whether authorised or not authorised or as a result of the negligence, 4. wilful misconduct, or 5. breach of any of the terms of this Agreement by User, (including but not limited to claims, liabilities, losses, damages, judgments and costs), 6. disruption to User's telephone services during the installation of an ADSL Service. Section 6.5: With the exception of obligations under the Broadband Guarantee Program, NetSpeed reserves the right to terminate any account at any time with or without cause or reason. In the event that NetSpeed would choose to take this action the User understands and agrees that the Users (sic) only compensation would be a prorated refund for the current period that User has already paid.

[241] The ACCC has recently conducted an audit of sorts of various industry terms and conditions, which resulted in many companies changing their documentation by consent: ACCC, 'Unfair Contract Terms- Industry Review' (2013 accessed 14 July 2014) http://www.accc.gov.au/publications/unfair-contract-terms This is a far less expensive form of regulatory activity and potentially achieves useful results in terms of targeting the bigger players, protecting a greater number of consumers, improving industry standards and sending out a message across the industry.

[242] ACL section 64. The section prohibits express terms which exclude, restrict or modify the guarantees or any term which is inconsistent with a guarantee. Note the effect of s 64A however.

[243] ACL section 51 (unless the supply is by hire or lease). In the circumstances of cloud computing, the terms and conditions are likely to dictate this aspect.

[244] ACL section 52 (only for the period of hire or lease).

[245] ACL section 53.

[246] ACL section 54.

[247] ACL section 55.

[248] ACL section 56.

[249] ACL section 57.

[250] ACL section 58.Note that these must comply with Regulation 90 of the Competition and Consumer regulations 2010 (Cth) which specifies a text which must appear, as well as mandates providing who provides the warranty, the duration and how to claim under it.

[251] The third guarantee is that services will be provided within a 'reasonable time' but it does not apply where there is a 'manner' for determining time frames agreed to by the consumer and supplier. It is likely most cloud provider contracts would cover this field.

[252] ACL section 60.

[253] ACL section 61.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

expect[,] to achieve that result …"[254] Given the nature of cloud services, it is arguable that by paid or free subscription (for example) a consumer is by implication, making known an expectation that the services and products will meet the service levels and performance promoted by the cloud provider. The courts have power to declare an unfair term void[255] and if a trader seeks to enforce that term, the courts may grant an injunction or compensate for or prevent loss or damage.[256]

In summary, there is potential doubt as to the application of consumer guarantees on two fronts: firstly whether 'free' services fall within the 'trade or commerce' requirement (which means they would not apply at all) and secondly, whether the specific form of cloud provision is a 'good' or 'service',[257] which will determine which (if any) guarantees are found to apply. As previously suggested, it seems likely that most cloud provisioning is a service, but software as a 'good' is discussed for completeness.[258]

4.2. *Other laws*

There are a wide range of consumer-protective laws which might apply in a cloud computing context, other than the ACL. For example: laws as to negligence, breach of contract, the *Electronic Transactions Act 1999* (Cth), state and territory laws governing minors who enter into contracts,[259] the *National Consumer Credit Protection Act 2009* (Cth), the Privacy Act 1988 (Cth) and the (non-binding) Australian Guidelines for Electronic Commerce.[260]

There "may [also] be circumstances"[261] where the *Telecommunications Act 1997* (Cth) Schedule 2 (**TA**) applies depending upon the products and services a cloud service provides: for example, a cloud system which enables data upload and storage is unlikely to be a defined 'carriage service' but a webmail service enabling user communication, may be.[262] Where this is the case, consumers may access the Telecommunications Industry Ombudsman (**TIO**)[263] complaints service under the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).[264] This is potentially an inexpensive and accessible private dispute resolution option, which is far easier than taking action under the ACL or state equivalents. However, given the technical uncertainty as to its application, it is unsurprising that here is no evidence that any complaint has been heard in this area to date.[265]

A cloud service provider may also be a "content services provider' under the TA, for example, where a pay TV service is provided using a listed carriage service.[266] Defined as "any online service", a content service is likely to include cloud services and is therefore subject to the relevant provisions governing this entity. As a content service provider or possibly, as an internet service provider, a cloud provider may also be caught by the *Broadcasting Services Act 1992* (Cth), as are internet content hosts which host internet content in Australia.[267] In this case, the cloud provider could fall subject to the regime administered by ACMA with respect to prohibited and illegal content.

These provisions are beyond the scope of this paper and clearly, they are only applicable to cloud service providers within a specific range of service offerings. ACMA has criticised the present disarray in its regulatory powers with respect to the cloud as a reflection of "broken concepts" in terms of the telecommunications regulation landscape generally.[268]

[254] ACL section 61(2).
[255] ACL section 250. Note that declarations may be sought by a contract party or the regulator (ACCC or state fair trading body).
[256] ACL s.232(3) and s.238(1).
[257] The question is presently before the Federal Court of Australia in *Australian Competition & Consumer Commission v. Valve Corporation* NSD 886/2014, where inter alia Valve argues that the proper law of the contract is that of the State of Washington, USA and secondly, that the provision of online access to video games is a 'service', not the provision of 'computer software' and therefore, not a 'good'. The ACCC has pleaded their case based upon the consumer guarantees pertaining to 'goods'. The case is set for court-ordered mediation on 1 April 2015 and failing a resolution, will proceed to trial on the issue of liability in July 2015. There is still doubt as to whether software constitutes a 'good' or 'service' in the UK and there are differing state findings across the US: See for example, Michelle Sherwood, 'Software: Goods or services?' *Shoosmiths* (24 Aug 2010 accessed 7 Aug 2014) <http://www.shoosmiths.co.uk/client-resources/legal-updates/Software-Goods-or-services-1193.aspx> One US decision says that a free software download is neither: Woffard, Lenox & Ors v. Apple Inc., Case No. 11-CV-0034 AJB NLS US District Court (Southern District of California) (8 Nov 2011) http://law.justia.com/cases/federal/district-courts/california/casdce/3:2011cv00034/341655/16 See also Sean Kalinich 'Judge Rules that Software is not a Good or a Service' *DecryptedTech* (13 November 2011 accessed 7 Aug 2014) <http://www.decryptedtech.com/editorials/judge-rules-that-software-is-not-a-good-or-a-service#bqE7TLBvqiVMuMlw.99>.
[258] One US decision says that a free (Apple iOS4) software update download is neither. Note however that the case turned on very narrow definitions within the relevant legislation as to what constitutes 'goods' or 'services' and the fact that a free upgrade did not fall under the relevant sale or lease laws: Woffard, ibid.
[259] For example, the *Minors (Property and Contracts) Act 1970* (NSW) and other state and territory equivalents.
[260] Department of Treasury, 'The Australian Guidelines for Electronic Commerce' (2006 accessed 4 Aug 2014) <http://archive.treasury.gov.au/contentitem.asp?ContentID=1083>.
[261] Australian Government, Department of Communications, 'Cloud Computing Regulatory Stocktake' Version 1 (May 2014 accessed 17 June 2014) [27] <http://www.communications.gov.au/__data/assets/pdf_file/0004/226930/Cloud_Computing_Regulatory_Stock_Take_-_May_2014.pdf>.
[262] Ibid: 28.
[263] See https://www.tio.com.au/. The TIO will pursue parties which ought to be signatories to ensure thy sign up.
[264] Regulatory Stocktake: above n 36: 28.They may also be bound by the *Telecommunications Consumer Protection Code* which covers areas such as advertising, privacy, point of sale information, billing and complaint handling.
[265] Author search of the Telecommunications Industry Ombudsman website https://www.tio.com.au/ on 10 August 2014 suggests that no complaints involving the 'cloud service providers' have been considered. Of course, it is not impossible that a case has been heard without that categorisation.
[266] *Telecommunications Act 1997* (Cth) s. 97.
[267] CC Regulatory Stocktake: Above n 36: 29.
[268] ACMA, 'Broken Concepts – A 2013 update on the Australian communications legislative landscape' (June 2013 accessed 7 Aug 2014) <http://www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/broken-concepts>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

4.3. *Cloudy cases & case scenarios*

In Australia, there are few consumer law cases concerning the cloud. This section therefore selects a miscellany of examples, from various jurisdictions, to show the type of litigation which consumers are starting to institute. It is not suggested that these cases constitute a coherent body of law, or that the matters would be decided the same way in Australia; rather, that these cases are interesting, illustrative and possibly, predictive of where Australian consumer law cases may go in the future.

Unfair terms have been perhaps the most fruitful source of cloud-related cases. On 13 May 2014, the Norwegian Consumer Council filed a complaint against Apple with their consumer ombudsman.[269] The complaint alleged a violation of European consumer law alleging that a clause permitting unilateral variation without notice in the Apple iCloud terms and conditions was 'unfair'.

Commentators suggest that this case will succeed, as it would be likely to do were it brought in Australia under the unfair terms regime. Another example which might potentially succeed here concerns the unilateral variation of terms and conditions. In 2012, Facebook conducted a study of almost 700,000 users which entailed secret and undisclosed 'emotional manipulation'. They subsequently changed their user terms in 2014, for the purposes (allegedly) of retrospectively covering up that they did not have sufficiently broad terms and conditions to authorise the study when performed, absent specific user consent.[270]

> *Some critics don't think that throwing the word "research" into a many-thousands-word-long data use policy is adequate for performing psychological experiments on users, but now it seems that Facebook hadn't even done that.*[271]

The matter has been referred to the US Federal Trade Commission, but it would be potentially arguable under unconscionability, false representations and misleading and deceptive conduct were the regulator to take action here.

There are many consumer class action cases taken against cloud providers in the US, many of which seem to be unsuccessful due to quirks in US laws. A recent US case which failed is *Woffard & Lennox v Apple Inc.*, in which the plaintiffs filed a class action law suit alleging that Apple's iOS 4.0 *iphone* software upgrade had impaired the functionality of their *iphone* applications utilising the AT&T network[272] in a manner recoverable under various Californian laws. The application was dismissed, inter alia, for reasons that the upgrade was 'free' and so not a "sale or lease'[273] and as software is not a 'good' under the relevant state laws.[274] Were such an application to be brought in Australia, and depending upon the nature of the damage sustained, whether conduct 'in trade or commerce' can be established and the nature of Apple's conduct (were there misleading or false representations as to product performance, for example or a breach of a consumer guarantee) then it is possible that there could be legal or ACCC-negotiated recovery. Likewise in the US, the *Comer* litigation accused Apple of "unfair, unlawful, deceptive and misleading practices" in promoting that iCloud was 'reliable' and 'simple'.[275] The complaint concerned the migration of Apple users from *mobileMe* to *iCloud* and alleges a lack of syncing ability, email functionality and other "complications and losses and corruption of data …"[276] Were these allegations proven, there seems little reason why the non-excludable consumer guarantees provisions would not apply, particularly in circumstances where paying subscribers were migrated at Apple's behest. G-mail has also been the target of numerous (unsuccessful) privacy-related class actions on the basis that it engages in the "systemic interception and use of electronic communications."[277] Copyright cases in the US still struggle with the cloud and its business models,[278]

[269] Forbrukerradet, 'Complaint regarding Apple's icloud's terms and conditions' *Case No 14/2842-1* (13 May 2014 accessed 11 July 2014) <http://www.forbrukerradet.no/_attachment/1175090/binary/29927>.

[270] Note there was also no capacity for facebook to exclude minors from its sample, which added to allegations that the study was unethical: Kashmir Hill, 'Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study' *Forbes* (30 June 2014 accessed 30 July 2014)< http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/>.

[271] Ibid. Hill.

[272] Order granting Motion to Dismiss, 8 Nov 2011 [3].

[273] As required under the *Consumer Legal Remedies Act* (California Civil Code §1750 et seq.) which refers to unfair or misleading acts undertaken by any person in a transaction intended to result in a sale or lease of goods or services to a consumer.

[274] *Ferrington v. McAfee, Inc.*, 10-CV-01455-LHK, 2010 WL 3910169 (N.D. Cal. Oct 5, 2010).

[275] *Comer v Apple Inc.* Case No. 12 2457, 15 May 2012 US District Court, Northern District of California (accessed 12 July 2014) <http://docs.justia.com/cases/federal/districtcourts/california/candce/5:2012cv02457/255082/1/0.pdf>.

[276] Neil Hughes 'Class-action suit targets Apple for iCloud downtime' (18 May 2012 accessed 12 July 2014) <http://appleinsider.com/articles/12/05/18/class_action_suit_targets_apple_for_icloud_downtime.html> The class action alleges violation of the Magnus-Moss Warranty Act, false advertising, express warranty breach, unjust enrichment, breach of implied warranty of merchantability and breach of the *Consumer Legal Remedies Act* (Cal).

[277] See for example, Scott v. Google Inc., US District Court, Northern District of Florida, Tallahassee Division, Civil Action No. 4:12-614 (28 Nov 2012).

[278] See for example, *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F. 3d 121, 87 U.S.P.Q.2d 1641, 2008 ILRC 2401, 25 ILRD 601, 36 Med. L. Rptr. 2185, 45 CR 989 (2d Cir. 2008) [2008 BL 162181] (Cablevision Case) which held that a digital video recorder system controlled remotely by users through their internet connection did not infringe the *Copyright Act* as it was a one-to-one performance – not one to the public per se. The case was hailed as enabling online services such as cloud storage with legal certainty. In contrast, the *Aereo* decision may overturn *WPIX v wvi Inc* which held that internet services cannot obtain a (compulsory) cable license as they are not a "cable service". See Matt Schruers 'Symposium: Aereo copyright decision creates uncertainty for the Cloud' *SCOTUSblog* (26 June 2014 accessed 30 June 2014) http://www.scotusblog.com/2014/06/symposium-aereo-copyright-decision-creates-uncertainty-for-the-cloud/.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

the latest incarnation being *ABC v Aereo*,[279] which held that a company "publicly performs" a copyright television program when it retransmits a free-to-air signal via subscribed user-controlled internet-connected antennas.[280]

Australia has seen several procedural cases of interest. The Qld Supreme Court has recently held[281] that service of legal documentation via a link to Dropbox was ineffective under the *Electronic Transactions (Queensland) Act 2001* as the Dropbox documents were not "… part of an electronic communication as defined. None of the data, text or images within the documents in the Dropbox were electronically communicated …"[282] The case does not involve a defect in Dropbox; but reveals how cloud technology is not yet an accepted form of service unless the parties contractually agree otherwise.[283] Other forms of litigation affecting cloud providers at the moment, are litigation-based. In the US, there have been several cases concerning cloud vendors and e-discovery; in *Sekisui*, where a company stores data in the cloud which is required for discovery purposes, the company is responsible to issue a litigation "hold" to the cloud provider, to prevent routine destruction of such documentation under a cloud services agreement.[284] Another scenario is search warrants which compel disclosure of customer personal data, often internationally. *In Matter of a Warrant to Search a Certain E-mail Account Controlled and maintained by Microsoft Corporation*[285] US orders were granted compelling disclosure of emails stored in Ireland, which would breach Irish or other EU data transfer laws - leaving Microsoft in a very difficult legal position. A similarly difficult legal situation is that posed by broad warrants which enable law enforcement to seize servers and thereby, adversely affect every company whose information might be cloud stored on those servers.[286]

The case highlights the risks of storing data in the cloud beyond its owner's control, which together with issues of cloud provider cessation of service,[287] bankruptcy, natural disaster or even sabotage, may adversely and possibly catastrophically, impact upon cloud consumers.[288]

5. Industry solutions? *Cloud code* is not one of them

Security professionals in general distrust the cloud—losing control, fly-by-night third party solutions, privacy and surveillance … [289]

[279] *American Broadcasting Companies, Inc. v. Aereo, Inc.* Docket No. 13-461, 2d Cir, 22 Apr 2014. The District Court and US Second Court originally found (inter alia) that Aereo's system did not infringe US copyright laws and the case went unopposed to the Supreme Court on appeal. The system gives subscribers access to **local** free-to-air broadcast television signals using an internet-connected device by accessing tiny, user-controlled remote antennas. Aereo regards itself an equipment (i.e. antennas) rental supplier. Broadcasters claim that this violates their *Copyright Act* public performance rights under section 106(4) of the US Copyright Act. The Supreme Court found 6 to 3 in their favour. The judgment was heavily criticized for adopting a "looks like" cable approach without investigating the technology, which resulted in "guilt by resemblance". It creates little certainty for those devising new technology: See Schruers, Ibid.

[280] Even though these broadcasts are 'free', cable providers must pay to retransmit broadcast signals – hence this revenue stream was threatened by the Aereo technology. An example is NFL broadcasts: Kang, Cecelia 'How the Supreme Court's ruling on Aereo could change how we watch football' *The Washington Post* (17 June 2014 accessed 19 June 2014) <http://www.washingtonpost.com/business/technology/how-the-supreme-courts-ruling-on-aereo-could-change-how-we-watch-football/2014/06/17/b314ca20-ea91-11e3-93d2-edd4be1f5d9e_story.html>.

[281] *Conveyor & General Engineering Pty Ltd v Basetec Services Pty Ltd* [2014] QSC 30.

[282] Section 11 includes communication by 'guided or unguided electromagnetic energy'. The court concluded: "Rather, there was an electronic communication of the means by which other information in electronic form could be found, read and downloaded at or from Dropbox website". Importantly, there had been no pre-agreement for electronic service under the Act, and as such, no form of e-service (cloud or non-cloud) would have sufficed.

[283] Tree, Jackson 'Lost in the Clouds: Supreme Court decision highlights risks of using cloud technology to serve documents' *Dibbs Barker Publication* (8 May 2014 accessed 20 June 2014) <http://www.dibbsbarker.com/publication/Lost_in_the_clouds__Supreme_Court_decision_highlights_risks_of_using_cloud_technology_to_serve_documents.aspx>.

[284] *Sekisui Am. Corp v Hart* 12-cv-3479, 2013 U.S. Dist. LEXIS 115533 (S. D.N.Y. 2013). The plaintiff was found to have destroyed electronically stored information of the defendants, and failed to issue a litigation hold (on destruction) to an offsite cloud provider in a timely manner, such that discoverable documents were lost. The appeals judge granted an adverse inference jury instruction and monetary sanctions against the plaintiff. This case suggested the cloud provider is the 'agent' of the email owner whereas a Singaporean case used the term "custodian": *Dirak Asia Pte Ltd and another v Chew Hua Kok and another* [2013] SGHCR 01 [12]. Either way, cloud consumers need to ensure clauses governing discovery and data extraction for litigation purposes are inserted into cloud service agreements.

[285] 13 Mag. 2814 per Judge James Francis IV cited in Rob Corbet, 'Microsoft and the US court — complying with US search warrants' 164(6) *Privacy & Data Protection* (2014 accessed 11 July 2014) <http://www.arthurcox.com/wp-content/uploads/2014/06/Microsoft-and-the-US-court-complying-with-US-search-warrants-Rob-Corbet-Arthur-Cox.pdf>.

[286] *Liquid Motors, Inc. v. Lynd*, No. 3:09-cv-0611-N (N.D. Tex. April 3, 2009).

[287] See for example, the demise of the storage system Ubuntu referred to earlier - "as of June 1st, 2014, syncing will stop. On July 31st, 2014, all data will be wiped. Ubuntu One will be no more": Wallen above n 32. Canonical (Ubuntu) refunded paid account fees to the date of the announcement, and offered to "try" to provide easy migration assistance: Jane Silber 'Shutting down Ubuntu One file services' *Canonical Blog* (1 April 2014 accessed 30 Aug 2014) <http://blog.canonical.com/2014/04/02/shutting-down-ubuntu-one-file-services/>.

[288] "The customers of cloud services face more than just the risk that police will confiscate a provider's servers. The provider may go into bankruptcy or suffer sabotage at the hands of a disgruntled employee. To address these risks, customers might spread or duplicate their data and services across multiple service providers, located in multiple jurisdictions.": Benjamin Wright, "Cloud Computing Police Raid' (22 Aug 2011 accessed 10 Aug 2014) <http://legal-beagle.typepad.com/wrights_legal_beagle/police-investigation/>.

[289] Philippe Courtot, 'The Cloud – Security Nightmare or Our Next Great Hope?' RSA Conference San Francisco, *Keynote* (February 27, 2014 accessed 7 July 2014) <http://www.rsaconference.com/videos/127/the-cloud-security-nightmare-or-our-next-great#sthash.l0n1yaFF.dpuf>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

Part 4 reveals that while Australian consumer law is generally in practice, an "alliance approach"[290] in the sense that the regulator, industry and consumer groups *should* have aligned interests in ensuring that consumer rights are protected, it seems that the cloud industry is not yet legally mature, responsive enough or sufficiently compliance-aware, to ensure that regulation and voluntary self-regulatory behaviours are largely aligned. The continued use of extensive and often one-sided terms and conditions – and their approach to code solutions discussed in this section – seems to evidence that issue.

5.1. *Codes & standards*

Cloud services in various forms may fall under many differing codes: the mandatory (where applicable) ASIC *ePayments Code*,[291] and the *Telecommunications Consumer Protection Code*,[292] and the voluntary Internet Industry Association *iCode*, *Content Services Code* and *Approved Vendor Trust Marque*. In addition, there is the voluntary New Zealand *CloudCode* and the voluntary UK Cloud Industry Forum's *Code of Practice*. There are also standards accreditation under numerous international security standards[293] and for-profit accreditation schemes such as *TRUSTe*. The Australian industry has most recently considered adopting the NZ *CloudCode*, so it forms the basis for the discussion as to code options in Part 5.2 below.

5.2. *CloudCode*

> *By setting a standard … the code makes sure that participating providers will give the right information to consumers to help them make good decisions. This is a very positive initiative … and I hope it will be widely adopted …* [294]

The cloud industry in Australia almost universally rejected devising a cloud computing consumer protocol or joining the NZ voluntary disclosure-based Cloud Computing Code of Practice (*Cloudcode*).[295] Albeit "… a code … that is easily adopted by the providers and easily understood by the consumer",[296] and despite promotion by the then federal government as a way to encourage cloud education, information dissemination and uptake by small business,[297] the response from the "major global cloud suppliers",[298] telecommunications providers[299] and peak industry bodies, was negative - such that a voluntary code would not be "viable".[300] Telstra, for example, argue that the Australian cloud market is robust, disputing the validity of "highly variable" research[301] as to SME uptake,[302] assert that there is no 'market failure' to justify a protocol, and that Australian consumer and privacy laws are superior to those in NZ and can address perceived (unproven) problems with 'cloudwashing'[303] for example. Likewise, Google state that a "highly prescriptive protocol" is inappropriate, given the dynamic nature of the IT industry[304] and that tech startups could be hurt by the protocol. The ACS Report, which

[290] Malbon coins this phrase to refer to the use of atomistic power to attain desired policy goals in a cooperative policy-aligned exercise between the regulator and those parties who exercise localised power sources: Justin Malbon, 'Taking Fake Online Reviews Seriously' *Journal of Consumer Policy*, (2012) 36:2: 139 -157 [153] <http://link.springer.com/article/10.1007%2Fs10603-012-9216-7#page-1>.

[291] ASIC above n 183.

[292] Registered in 2012, ACMA describes this Code as better consumer protection against "bill shock, confusing mobile plans and poor complaints handling". Urgent matters are dealt with within 2 days. It is apparent from the ACMA website that the regulator's focus is the mobile phone industry, rather than cloud providers: ACMA, The TCP Code (undated accessed 10 Aug 2014) <http://www.acma.gov.au/Industry/Telco/Reconnecting-the-customer/TCP-code/the-tcp-code-telecommunications-consumer-protections-code-acma>.

[293] Telstra cites the following examples of cloud standards in its ACS submission: ITU, ISO, OASIS, CSA together with best practice Cloud Controls Matrix and Cloud Trust protocol: Telstra Corporation Limited, 'Cloud Computing Consumer protocol Response to ACS Discussion Paper' *Submission* (19 Aug 2013 accessed 16 June 2014) <https://www.acs.org.au/__data/assets/pdf_file/0020/21881/4-Telstra-submission-ACS-Cloud-Computing-Consumer-Protocol-19-Aug-2013.pdf>.

[294] Marie Shroff, 'Privacy Commissioner's Annual Report 2013: a Year of Rapid Change' <http://www.privacy.org.nz/news-and-publications/statements-media-releases/annualreport2013/>.

[295] Above n 1.

[296] Istart, 'Aus lags NZ with cloud computing industry code of practice' (undated accessed 17 July 2014) <tttp://www.istart.com.au/index/HM20/AL211017/AR213670>.

[297] Australian Computer Society, 'Cloud Computing Consumer Protocol' ACS Cloud Discussion Paper (July 2013 accessed 6 June 2014) <http://www.acs.org.au/__data/assets/file/0018/21672/ACS-Cloud-Discussion-Paper.pdf>.

[298] Ibid: 3–4. Note that Amazon did not participate.

[299] Telstra for example, argues that the cloud market is robust and there was no 'market failure' to justify a protocol, and that Australian consumer and privacy laws are superior to those in NZ: Telstra, above n 293.

[300] The consultation process involved 23 written submissions and around 400 attendees at workshops across four capital cities: Australian Computer Society, 'ACS Cloud Protocol Consultation' Report on the outcome of the ACS Public consultation on Cloud protocol (11 Nov 2013 accessed 6 July 2014) <http://www.acs.org.au/__data/assets/pdf_file/0017/27800/ACS-Cloud-Protocol-Consultation-Report.pdf>.

[301] Above n 293. Telstra dispute security of data offshore concerns raised by ACMA as "from an unpublished study" but do acknowledge that there may be a consumer confidence problem – but this is in their view, unproven.

[302] Telstra cite Springboard group research which indicated 19% small business and 31% of SMEs had adopted cloud computing versus Frost & Sullivan which found that 43%: Ibid: 5.

[303] This term covers misrepresentation of non-cloud offerings as 'cloud computing'. It is unclear as to the extent of this problem, and no evidence is provided by the Institute of IT Professionals (which drafted the Code) as to its prevalence. As it seems a major thrust of the *CloudCode*, it is presumably perceived as a significant issue within the New Zealand industry. Of course, cloudwashing is likely to be a misrepresentation actionable under the *Australian Consumer Law* both for misleading and deceptive conduct (s. 18) and false misrepresentations (s. 29).

[304] Tim Lohman 'Google, Telstra, Microsoft rail against cloud regulation' *ZdNet* (30 Aug 2013 accessed 10 Aug 2014) <http://www.zdnet.com/google-telstra-microsoft-rail-against-cloud-regulation-7000020039/> citing Google Inc., Google Inc., 'Discussion paper: Cloud Computing Consumer protocol' (Aug 2013 accessed 10 Aug 2014) <http://www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol/2013-australian-cloud-protocol-submissions>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

ultimately recommends an education process while observing the *CloudCode* performance, reiterates the Telstra case almost entirely. This is despite extensive submissions by consumer groups arguing for a mandatory regulatory process, on the basis that voluntary self-regulation will be not effective.[305] It is difficult not to construe this outcome as indicative of an industry with little respect for its consumer disclosure obligations and even less for self-regulation.[306]

It is also difficult not to construe the various cloud code offerings as relatively weak[307] – compared to other industry self-regulatory codes. *CloudCode* is evaluated in Annexure Four [Available online as "supplementary material" on ScienceDirect] by reference to the Australian Self-Regulation Best Practice model.[308] As the evaluation reveals, *CloudCode*[309] is an innovative self-regulatory code whereby cloud service providers commit to uniform template[310] disclosure,[311] as well as submit to a very limited, code-prescribed complaint resolution process. It succeeds insofar as it offers a rigorous standard-form disclosure regime which forces providers to address significant cloud service and contractual 'issues' for consumers, such as privacy, security, data transportability and the like.[312] It thereby enhances consumer understanding of products and enables a comparative "informed decision". It also succeeds in importing providers' legal obligations through three broad (country-specific) disclosures: firstly, a signatory must affirm that it "… will always comply" with relevant (specified) laws as to privacy, fair trading etc.[313] Secondly, they must disclose their fair trading compliance program (if any) and thirdly, a signatory must disclose whether it offers data breach notification in accordance with the NZ Privacy Commissioner's voluntary (privacy) breach notification guidelines.[314]

However, *CloudCode* fails dismally in its disputes resolution process by reference to the DIST benchmarks,[315] which is a serious deficiency. The dispute resolution procedures are minimalist, lack formal controls and useful sanctions and generally, do not represent a serious form of consumer dispute resolution other than for the purposes of code administration. It is implicit within the Code that disgruntled consumers are left to pursue traditional legal avenues of redress rather than relying upon the Code, in most (if not all) instances of alleged Code breach. The Code does regulate 'false and inaccurate' disclosures, but offers no consumer redress even where a complaint is upheld. The formal dispute resolution processes are not prescribed which raises questions of potential bias and procedural fairness issues, and there seems little motivation for any consumer to complain, given the best possible outcome is rectification of a disclosure statement or the expulsion of a provider from the Register. Neither of these offer a consumer any personal redress. Given this deficiency, it is scarcely surprising that there have been no complaint determinations to date.[316]

So while the Code is not qualitative, legally binding or prescriptive in terms of specifying standards to which signatories must adhere, it does operate to promote or encourage practices which are consumer-friendly by exposing service deficiencies and creating binding written representations on the big ticket cloud terms. But the enforcement regime is through adherence to existing laws[317] and compliance options, rather than through onerous sanctions or penalties under the code itself.

[305] See for example, the 19 recommendations from Australian Communications Consumer Action Network (ACCAN), many of which point to deficiencies in the NZ *CloudCode* on the basis that it is too industry-friendly: ACCAN, 'Cloud Computing Consumer Protocol: Submission by the Australian Communications Consumer Action Network to the Australian Computer Society' (16 August 2013 accessed 6 June 2014) <http://www.acs.org.au/__data/assets/pdf_file/0006/21894/12-accan_sub_acs_cloud_protocol.pdf>.

[306] The ACS report that the 'knowledge gaps' concern stems from consumer and SME issues: i.e. "they lack the time and resources to gather the information they need to address any contractual or poor performance issues with suppliers": Ibid: 4.

[307] For example, see CloudCode and the Cloud Industry Forum 'Code of Practice' for Cloud Service providers.

[308] Australian Government Taskforce on Industry Self-Regulation, *Industry Self-Regulation in Consumer Markets – Final Report* (1 Aug 2000 accessed 9 Mar 2014) <http://archive.treasury.gov.au/documents/1131/PDF/2part1.pdf>.

[309] Above n 1.

[310] *CloudCode*, 'Template' (undated accessed 16 July 2014) <https://www.thecloudcode.org/BecomeaSignatory>.

[311] *CloudCode* section 5.

[312] The disclosure document includes legal matters such as the governing law (cl. 1), ownership of data/information and metadata/statistical information,(cl. 2) security standards (physical and digital),(cl. 3) primary system and backup data location, (cl. 4) data access post contract or by law enforcement agencies (cls. 5 and 15), geographic locations of servers, (cls. 6 and 7) support and service level requirements, (cl. 8) incident response and reporting, (cl. 8) data transportability, (cl. 9 which mandates disclosure of whether or not data will be available to download after service supply ceases as well as any additional access charges); business continuity, (cl. 10. This requires the service provider to state their business continuity preparations as well as arrangements of any upstream provider); data formats and application ownership, (cls. 11 and 12) data breach (cl. 14) and region-specific disclosure. (cl. 16). The latter specifies New Zealand specific content and presumably, is designed for other countries to specify equivalent applicable legislation.

[313] Ibid: schedule 1 'New Zealand Specific Content'. The specified laws are the NZ *Privacy Act 1993*, *Fair Trading Act, Commerce Act, Copyright (infringing File Sharing) Amendment Act* 2011 and "other relevant legislation".

[314] New Zealand Privacy Commissioner, 'Privacy Breach Guidelines' (2008 accessed 16 July 2014) http://www.privacy.org.nz/news-and-publications/guidance-notes/privacy-breach-guidelines-2/.

[315] These are used both in Australia and New Zealand in the financial and credit industries which must have a compliant dispute resolution system to handle consumer complaints: Commonwealth Consumer Affairs Advisory Council, 'Review of the Benchmarks for Industry-based Customer Dispute Resolution Schemes' (24 April 2013 accessed 11 Aug 2014) [12–13] <http://ccaac.gov.au/2013/04/24/review-of-the-benchmarks-for-industry-based-customer-dispute-resolution-schemes>.

[316] Email to author from Joy Cottle, Operations Manager, Institute of IT Professionals NZ dated 11 Aug 2014.

[317] Cloud Code, above n. 1: clause 3.2.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

In summary, this assessment reveals that consumer protection conferred by the *CloudCode* by way of disclosure is positive but ultimately laissez-faire, and its dispute resolution process is minimal and non-transparent, consistent with the ambitions of the Code in that regard. Given its largely unthreatening nature, it is therefore very difficult to understand why the Australian cloud industry was so resistant to joining a code that could only enhance transparency and consumer confidence in their industry.[318]

6. Where to this cloud?

> *We fundamentally blindly trust … [w]e trust licensing, we trust litigation, there's a lot of systems we have for when trust fails. All these critical apps are a very human system, and thanks to the cloud, computing is moving back toward trust.*[319]

> *"It's not an all-or-nothing strategy," Feigenbaum said. He described three kinds of data that most companies produce: public data, sensitive data, and top secret data. The first two, he said, are acceptable for the cloud, but things like system requirements and public infrastructure should be kept off the cloud for now.*[320]

6.1. An inevitable scenario … ?

Case law evidence suggests that Australian consumers are either not feeling cloud computing concerns, or are not as yet disposed to complain about them. There are few legal cases, few records of complaint to the regulators and scant evidence that cloud consumers are dissatisfied with their experience.

But while incident levels may be relatively low, the risk profile of cloud computing is according to security experts, high.[321] There have already been serious security breaches, data loss and outages as discussed. It is not inconceivable that eventually, a cloud service will suffer a major or even total collapse – and all its customer data be irretrievably lost, stolen or publicly disclosed. The potentials for criminal misuse, as well the consequences for service users (who may for example store everything in the 'cloud' without backup) are potentially disastrous. And the technical threats are real: hardware failure, natural disaster, service closure, cloud-related malware and inadequate infrastructure planning are all factors which may lead to cloud service collapse.

It therefore seems likely that a major cloud service collapse of some sort or another, in inevitable. The question, is will appropriate regulatory settings will be in place to manage such a situation, and will the law offer consumers redress for this potentially destructive event.

6.2. Rethinking cloud regulation

> *The ACCC will be closely watching key areas of interest as cloud computing becomes more widespread. The … aim in consumer protection regulation is to ensure that consumers can benefit from innovation and competition through minimising the impact of market failures, information problems and rogue traders …* [322]

Traditional regulatory models and existing regulation are challenged by the rapidly growing, technology-driven and international nature of the cloud computing environment. Cloud service products blend that which Australian media and communications laws traditionally regulate separately: infrastructure, services and content.[323] In 2013, in reviewing this situation, the ACMA concluded that cloud regulatory implementation is "immature" and that there would be benefits in a "single coherent regulatory framework".[324]

The ideal of a single regulatory framework is both ambitious and challenging. In terms of extant consumer law, the ACL should be amended to overcome any uncertainty as to its application to cloud services under the consumer guarantees laws which apply somewhat awkwardly – both to software as a good and (less so) to cloud provisioning as a service. While it would be possible to insert provisions governing cloud-specific standards where the existing guarantees are not industry-relevant, a better option is to devise a mandatory industry code, which may be government-prescribed as an industry code of conduct and thereby enforceable under the Act.[325] The other option is to declare cloud providers as a section of the telecommunications industry under the TA, such that the ACMA could direct the cloud industry to develop a code, which can then be registered and enforced by the ACMA. Either way, the advantage is that a code is more industry specific and adaptable to change than legislation, and enables genuine industry buy-in. Of course, the cloud industry has already resisted a very moderate version of this, but were government to threaten enforced regulation, it seems likely that an industry-devised code will become a far more attractive prospect.[326] But even were these changes to occur, it is possible that the regulatory structure may never entirely 'keep up' with the constant evolution of cloud computing.

[318] Lohman, above n 4. Note there is also the Internet Industry Association's "iCode" which covers cybersecurity for ISPs and now covers 90% of that market: AII, "iCode" (1 June 2010 accessed 16 July 2014) <http://iia.net.au/userfiles/iiacybersecuritycode_implementation_dec2010.pdf>.

[319] Bruce Schneier, independent security analyst quoted in Rosenblatt above n 29.

[320] Eran Feigenbaum, Google Director of Security for Google Apps quoted in Rosenblatt, above n 29.

[321] It is hard to imagine more authoritative sources than those discussed in Rosenblatt: above n 29.

[322] Kell, above n 187.

[323] ACMA, above n 61.

[324] Ibid.

[325] See section 51AE of the *Competition and Consumer Act 2010 (Cth)*.

[326] For code development guidelines, see ACCC, 'Guidelines for developing effective voluntary Industry Codes of Conduct' (2011 accessed 16 July 2014) <http://www.accc.gov.au/publications/guidelines-for-developing-effective-voluntary-industry-codes-of-conduct>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

An 'alliance' regulatory approach[327] would propose a range of complementary regulatory mechanisms to capture cloud innovation while protecting consumers. These might include the following:

* Government promotion of industry self-regulation. The *CloudCode* is imperfect, but a start to developing the culture of greater industry accountability. It is apparent that the industry needs to proactively address issues of consumer education, information and disclosure; and to address deficiencies in consumer trust, whilst maintaining its capacity to respond to industry changes. A flexible and responsive self-regulatory system would be a positive fillip to this, as well as raising industry standards generally and increasing engagement with both consumer groups and the government.[328]
* Consumer and small business education: the ACS *Cloud Protocol Consultation* reported that all stakeholder groups supported an education campaign to define cloud services, outline potential benefits, identify extant consumer protection; inform as to cloud risks and benefits, and to suggest key purchaser questions to put to suppliers during procurement.[329]
* Current EU proposals to develop model 'safe and fair' contract terms and conditions[330] offer a positive approach to redressing existing issues with widespread standard form terms and conditions which are in many cases, unfair. The EU terms are to regulate specific cloud issues only[331] – and are subject to consumer group criticism as a "missed opportunity" for insufficient focus on ACL-type issues.[332] An Australian model might take a more comprehensive approach.
* Consistent with Code approaches to improving industry disclosure and consumer information, one of the most pressing requirements for the cloud industry is improved disclosure and a system of either voluntary or mandatory reporting of cloud outages and their causes.[333]
* Regulatory enforcement: the ACCC can readily obtain and review the contract terms of the cloud computing industry in Australia, and take enforcement action where necessary in the interests of industry education and consumer redress.[334] This process might also inform a standard industry model. Depending upon the results of the ACCC review, appropriate recommendations could follow as to making such a contract mandatory[335] or voluntary.

Finally, the ACCC could also institute a case to pursue a precedent in the courts as to the application of the ACL unfair terms provisions to consumers using supposedly "free" cloud services, as well as instituting proceedings to establish that privacy terms must comply with the relevant legislation and also not be unfair. The ACCC should also continue its lobbying for the extension of those same provisions to small businesses.

It is suggested that an alliance approach of this sort is the best possible approach to cloud regulation in Australia at this time.

6.3. *Some present political realities*

This paper evidences the rapidly-evolving practical realities of consumer: cloud industry interaction from a consumer law perspective. The Australian *Office of Best Practice Regulation* suggests that government intervention is appropriate where a policy problem arises due to (inter alia) market or regulatory failure[336] which is an idea explicitly rejected by the cloud industry. Further, the present Australian Government has a policy position against sector-specific legislation unless there is a demonstrable net benefit to the community.[337] Given this and the absence of any new national cloud computing strategy, the development of simplistic educational materials to promote cloud usage to SMEs and others, as well as the industry attitudes

[327] Justin Malbon, above n 290:151. He coins this phrase to refer to the use of power to attain desired policy goals in a cooperative policy-aligned exercise between the regulator and parties with localised power sources.

[328] "Self-regulation is a flexible response to market failure and may fill a 'gap' quickly and efficiently": Australian Government Taskforce on Industry Self-Regulation, *Industry Self-Regulation in Consumer Markets – Final Report* (1 Aug 2000 accessed 9 Aug 2014) [51] <http://archive.treasury.gov.au/documents/1131/PDF/2part1.pdf>.

[329] ACS Report above n 300:4.

[330] European Commission, 'Unleashing the Potential of Cloud Computing in Europe' Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions (27 Sept 2012 accessed 8 June 2014) <http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm>.

[331] Such as data preservation upon contract termination, data location and transfer, data disclosure and integrity, data ownership, direct and indirect liability, service change and subcontracting: European Commission, 'European Cloud Computing Strategy' (2012 accessed 11 June 2014) <https://ec.europa.eu/digital-agenda/node/10565>.

[332] BEUC describe the regulatory dilemma as "addressing a series of cross-cutting issues in multiple areas such as data protection, copyright or consumer protection and contract law, all the while providing for a neutral internet": BEUC, 'EU Cloud Computing Strategy' *BEUC Position Paper* (28 Feb 2013 accessed 11 July 2014) <http://www.beuc.eu/publications/2013-00143-01-e.pdf>.

[333] Ryan KL Ko, Stephen SG Lee and Veerappa Rajan, 'Understanding Cloud Failures' *IEEE Spectrum* (28 Nov 2012 accessed 2 Aug 2014) <http://spectrum.ieee.org/computing/networks/understanding-cloud-failures>.

[334] The first Victorian unfair terms case resulted in telecommunications provider AAPT redrafting its standard terms and conditions, and applying the revised document retrospectively: *Director of Consumer Affairs v AAPT Limited* [2006] VCAT 1493.

[335] See for example the BEUC view that an optional model pushes consumer protection to the "point of absurdity" – allowing industry choice through a voluntary system is absurd when (they assert) the industry has exploited current legal uncertainties and used unfair, non-transparent contracts: above n 332.

[336] Stocktake: above n 36.

[337] Department of Prime Minister and Cabinet, 'The Australian Guide to Regulation' (March 2014 accessed 21 July 2014) [2] <http://www.cuttingredtape.gov.au>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

discussed above,[338] it seems unlikely that cloud computing will be further regulated during this term of government.

7. Conclusion

Clearer and more consistent regulation would benefit consumers and industry alike and help make Australia a more competitive jurisdiction.[339]

Cloud computing is a phenomenon which is here for the long term and offers a vast array of benefits to consumers and businesses alike.[340] It has perhaps been oversold in terms of its present security and privacy capabilities: various predicted disasters have occurred but been managed and general confidence as to its security and privacy levels remains a legal and marketing vulnerability. It also exhibits a low level of understanding of industry to consumer ACL obligations and its contracting practises evidence this flaw. Despite these weaknesses, the industry is, save for the New Zealand example, slow to react and respond. This paper has sought to evidence that the future of the consumer cloud lies in creating a consumer law friendly environment. Suggestions such as industry code development, improved disclosure practices and the creation of consumer-law compliant contractual terms, will greatly improve the marketability and reputation of the cloud. Of course such changes would carry the corollary of greater legal accountability – and the increased possibility of consumer law enforcement by both regulators and consumers. But the cloud should both be big enough, resilient enough – and 'complianced' enough – to adapt to that rather small challenge.

It's time, at least in terms of consumers and consumer law, that the cloud – and cloud providers – grew up.

Acknowledgement

The author is LLM LLB (Hons) BA(Hons) (Melb), Teaching Fellow & SJD Candidate.

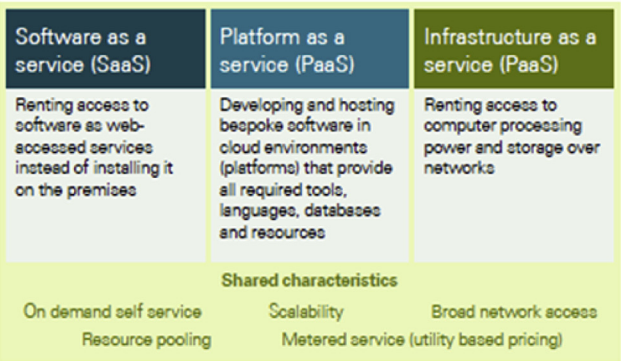
[338] The CC Regulatory Stocktake notes that industry stakeholders argue that further regulation at "a relatively early stage' could detrimentally affect competition in the cloud services market: above n 36: 66. As to the current government's approach, see the Department of Communication's materials intended to promote cloud to SMEs here: http://www.digitalbusiness.gov.au/tools/cloud-computing/.

[339] Above n 36: 66.

[340] The most commonly espoused business benefits are reduced IT costs, scalability, business continuity, collaboration efficiency work practice flexibility and access to automatic updates: Queensland Government, 'Cloud computing for business' (22 May 2014 accessed 7 June 2014) <http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

Annexure One. Cloud service offerings & deployment models (KPMG) [341]



There are four deployment models for these cloud service offerings: Private, Public, Community and Hybrid. The features and benefits associated with each are shown in Table 1 below.

Table 1: Cloud deployment models

Cloud type	Features	Benefits
Public	For use by multiple organisations (tenants) on a shared basis and hosted and managed by a third party service provider. Computing resources accessed as external services, instead of as products that are purchased, installed and managed within an organisation.	Ability to rapidly scale the allocation of computing resources to match fluctuations in business demand. Utility-based pricing, so that users only pay for computing resources actually used (rather than full load capacity). Potentially large economies of scale.
Private	For exclusive use by a single organisation and typically controlled, managed and hosted in private data centres. The hosting and operation of private clouds may be outsourced to a third party service provider, but a private cloud remains for the exclusive use of one organisation. Currently, the most common form of cloud in Australia, and typically the first step in a company's cloud journey.	Considered the most secure option, but with reduced potential for economies of scale and productivity gains available through multi-tenant options.
Community	For use by a group of related organisations that wish to make use of a common cloud computing environment for example, local councils with a shared service offering. Effectively half way between private and public clouds.	Reduced economies of scale traded off for increased security.
Hybrid	Both private and public cloud models are adopted by a single organisation.	Allows for multiple deployment methods to meet specific business/agency needs.

[341] KPMG, 'Modelling the economic impact of Cloud Computing' *Report to Australian Information Industry Association* (2012 accessed 14 July 2014) <www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf>.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006

Annexure Two. Simple Cloud Glossary[342]

ACCC: Australian Competition and Consumer Commission, an independent statutory authority which regulates competition, consumer protection and other laws under the *Competition and Consumer Act 2010* (Cth)
ACMA: Australian Communications and Media Authority, an independent statutory authority which regulates telecommunications service providers (carriers, carriage service providers and content services providers) in Australia
Cloud bursting : where businesses use cloud services to meet demand spikes, that is, to augment existing infrastructure and to avoid maintaining unused capacity
cloud service provider: a business which provides cloud services to consumers and others
cloud washing: where a vendor seeks to rebrand an old (or slightly re-tweaked)[343] product or service by associating it with the 'cloud'
community cloud: a cloud service which allows users with common interests or needs to share cloud infrastructure
consumer: individuals, SME and not-for-profit consumers excluding listed companies
data portability: the ability to move data stored on one cloud service to another or out of the cloud
elastic computing : is "the dynamic allocation of IT resources" whereby a user may buy cloud use for a limited period which is then shared with others for the remainder of the time.
hosting stack : refers to the cloud computing hierarchy of service layers – *IaaS*, *PaaS* and *SaaS* – the further into the stack, the more the cloud does for the user.
hybrid cloud service: a mixed public, private and community cloud service
IaaS: means using the cloud for things such as processing, storage, memory and networking. It saves businesses having to buy and look after expensive infrastructure.
ICT: information and communications technology
interoperability: the capacity of systems to interact with each other
NIST: National Institute of Standards and Technology (US Department of Commerce)
OIAC: Office of the Australian Information Commissioner, the regulator or privacy and freedom of information empowered to enforce the *Privacy Act 1988* (Cth) and for compliance purposes, under the *Telecommunications Act 1997* (Cth)
private cloud service: a cloud provided for the sole use of one entity which may be owner and operator by that entity or by a third party provider
public cloud service: a cloud provided by internet via shared infrastructure, usually with data and services hosted from different locations around the world
resilience: the ability of a service or network to continue to perform in the event of a service disruption
PaaS: platform as a service, which means a service providing a platform and tools for software developers to create and launch their own applications (e.g. Microsoft Azure and Force.com).
public cloud: a computing network spanning many countries/locations which offers applications and storage to the public over the internet.
SaaS: software as a service, which means internet-accessed software and applications which do not require installation and are updated by the provider, unlike most desktop applications (e.g. facebook, Google docs etc)
utility computing : means pay-as-you-go for the use of applications and software, rather than the user installing and maintaining them
vendor lock-in: where switching costs may inhibit a customer from leaving a cloud service provider, usually for reasons such as the cost of changing providers, adverse contractual terms or technical difficulties such as data portability or interoperability

Appendix A. Supplementary data

Supplementary data (Annexures 3 and 4) related to this article can be found at http://dx.doi.org/10.1016/j.clsr.2015.05.006

[342] Many of these definitions are derived in part from the terminology section of the Australian Government, Department of Communications, 'Cloud Computing Regulatory Stocktake' Version 1 (May 2014 accessed 17 June 2014) [6] <http://www.communications.gov.au/__data/assets/pdf_file/0004/226930/Cloud_Computing_Regulatory_Stock_Take_-_May_2014.pdf>.
[343] Gabriella Griffith, 'Jargon Buster' *Raconteur* (11 July 2013 accessed 2 June 2014) http://raconteur.net/technology/jargon-buster.

Please cite this article in press as: Mathews Hunt K, CloudConsumer: contracts, codes & the law, Computer Law & Security Review (2015), http://dx.doi.org/10.1016/j.clsr.2015.05.006