ARC Centre of Excellence in Policing and Security

Australian Government
Australian Institute of Criminology

Final Report – Cloud Computing Threat Assessment for Small Business

Prepared by the Australian Research Council (ARC) Centre of Excellence in Policing and Security (CEPS) and the Australian Institute of Criminology (AIC) for the Department of Broadband, Communications and the Digital Economy (DBCDE)

November 2012

Lachlan James, Alice Hutchings and Russell G Smith

The views expressed in this report are those of the authors alone and do not necessarily reflect the opinions or policies of the Australian Government or its agencies.

Small Business & Cloud Computing Threat Assessment

1 Executive Summary

Small businesses are not simply scaled-down versions of big business. Compared with larger organisations, small businesses operate in a distinct and highly resource constrained operating and technical environment. They are time-poor, have minimal bargaining power, and limited or inconsistent financial, technical, legal and personnel resources. Above all, small businesses are typically focused on one thing: survival. It is therefore unsurprising that cloud computing—and its promise of smoothing cash flows and dramatically reducing IT overhead—is attractive to small business.

Cloud computing shifts the delivery and maintenance of software, databases and storage to the internet, transforming them into Pay-As-You-Go (PAYG) services accessed through a small business user's web-browser. Cloud computing often comes with zero upfront costs, and scales (up and down) with the demands of the small business. Cloud computing services demand minimal technical skills: they are easy to setup and require little if any maintenance. Accessed via a secure login, for the small business, cloud computing typically represents increased standards of security.

However, along with the benefits, cloud computing also embodies many risks for small business, including potential computer security, criminal, regulatory and civil liability issues. Cloud computing—like other new information technologies—challenges the application and understanding of many pre-existing areas of law.

Key Criminal, Regulatory & Legal Threats for Small Business

Examples of key criminal, regulatory and legal threats for small business adopting cloud computing include:

- *Cloud Providers are the Target, But Small Business is the Victim* – While cloud service providers themselves hold much greater appeal to cybercriminals, it is the cloud service provider's small business tenants—experiencing disrupted services and hence disruption to their already fragile revenues—that are the real victims. Lacking policies, procedures and training relating to cyber and network security, small businesses are particularly vulnerable to having account details stolen, and their cloud services hijacked.
- *Ever Changing Sea of International, National & Local Regulation* – Where personal information—including financial and credit details—is stored in the cloud, a routine international commercial transaction may require a small business to comply with a myriad of ever changing international, national and state-level regulations and industry-specific standards.
- *Practical Benefits of Cloud Computing Potentially Non-Compliant* – Even some simple, practical benefits of using the cloud—such as storing MYOB files on a cloud storage service (such as DropBox)—may render the small business non-compliant.
- *Inequality of Bargaining Power: "Take It or Leave It" Service Agreements* – With almost no bargaining power and faced with industry-wide boilerplate terms and conditions, small business has little choice but to accept one-sided cloud agreements on a "take it or leave it" basis, leaving vendors absolved of substantially all liability.

- *Service Credits Inconsistent with Potential Damage to Small Business* – Despite the potentially devastating impact of even relatively short service outages, small business is typically left with "service credits" (based on a proportion of monthly subscription fees) as their "sole and exclusive remedy."
- *Overseas Legal Jurisdiction & Choice-of-Law* – With cloud service agreements frequently setting the legal jurisdiction and choice-of-law to the vendor's overseas headquarters, even the most simple legal action immediately becomes prohibitively expensive for all but the most successful small business.
- *Unilateral Termination of Accounts & Data Loss* – Cloud service providers, particularly in relation to free accounts, often reserve the right to unilaterally terminate accounts with or without notice, potentially devastating the small business. Absolved of substantially all liability, the cloud service provider leaves the aggrieved small business with no cause of action and no right to recover.

Findings – Responding to the Criminal, Regulatory & Legal Threats

Technical & Commercial Practices to Reduce Risks – The research has found that there are technical and commercial practices that can be implemented today by small businesses to reduce at least some of the security and commercial risks:

- *Policies & Training* – Small businesses can provide computer security training to personnel, and institute simple policies setting out (for example) how computer resources should be used, how often passwords should be changed, access rights for staff, and how and when employees may bring in and use their own devices.
- *Industry Education* – Industry bodies can provide education and training to small businesses about appropriate practices and regulatory requirements.
- *Cyber & Cloud Insurance* – Existing cyber liability insurance holds out some limited hope of compensating for losses as a result of cybercrime. However, the best hope for broader coverage rests with contingent business interruption insurance adapted to the unique circumstances of cloud computing ("cloud insurance") being developed by new entrepreneurial ventures such as CloudInsure.

Opportunities for Legislative Intervention – The research also identified the likely need for legislative intervention. The near-term future of cloud computing shows signs of bifurcation into budget solutions (much like existing offerings) and premium services with increased security and regulatory compliance, and greater acceptance of liability. But without a change in relative bargaining power between the cloud service provider and small business, it is unclear if competitive forces alone will be sufficient to bring about quality premium services at a price affordable to cost-conscious small business.

To encourage cloud service providers to deliver more attractive, secure and cost effective solutions, inequality of bargaining power between cloud service providers and small business clients will need to be addressed. In this respect, there is significant opportunity for judiciously applied legislative intervention. Opportunities for such carefully considered intervention include: a refined doctrine of unconscionability; possible introduction of legal principles broadly akin to "contracts of adhesion" in the United States; and new regulatory powers—possibly adapted from

the Communications Alliance (formerly the Australian Communications Industry Forum, Industry Code for Consumer Contracts, ACIF C620:2005)—to police the cloud computing industry.

Acting in concert, a combination of technical and commercial solutions—including improved cybersecurity practices, industry education programs, and new species of "cloud insurance"—together with legislative programs may serve to place small business on substantially the same footing as larger businesses, enabling them to fully capture the true benefits of cloud computing while enduring a more equitable share of the risks.

2 Introduction

The Department of Broadband, Communication and the Digital Economy (DBCDE) contracted the ARC Centre of Excellence in Policing and Security (CEPS) to conduct a cloud computing threat assessment for small business, a proposal jointly developed between CEPS and the Australian Institute of Criminology (AIC).

Based on desk-based research, this report aims to enumerate and clarify the current understanding of the potential criminal, regulatory and legal threats of small business seeking to adopt and benefit from cloud computing.

The report that follows discusses and expands on the threats of cloud computing to small business and outlines a way forward for small businesses to reduce those risks.

3 Research Aims

The aims of this research paper are to:

- identify the sources of potential benefits and risks to small business (compared with larger organisations) of cloud computing;
- identify criminal, regulatory and legal risks for small business;
- quantify the effect of cloud computing on computer and data security for small businesses;
- examine the potential for small businesses to rely on existing business insurance to compensate for cloud-related losses; and
- to identify whether it is necessary or appropriate to consider a new regulatory response for cloud computing providers and small businesses, or whether the existing regulations are appropriate.

The overall objective of this report is to: contribute to a more commercially secure business environment; identify and create awareness about the security, regulatory and legal considerations in relation to the uptake of cloud computing; and enhance small business's confidence in using cloud computing specifically, and the digital economy more generally.

4 Methodology

This report presents the findings of a desk-based assessment of English-language, public source literature available over the internet and through subscription-based services to identify current and emerging cloud computing risks and incidents, particularly in relation to small businesses of fewer than twenty employees.

The current report is a joint research project between CEPS and the AIC, with the following responsibilities:

- ***Small business and criminological threats*** – The AIC was tasked with detailing the criminological threats to small business users of cloud computing, including a review of computer security and criminological risks associated with cloud computing, computing security and criminological issues likely to arise over the next two years, and how cloud computing threats are being addressed by small business and cloud providers (see section 4).
- ***Small business and regulatory & legal threats*** – CEPS had responsibility for examining issues around small business and cloud computing in the context of regulatory compliance and civil legal matters, including a review of cloud service provider agreements, the potential of insurance to cover cloud-related loss, the use of third party IT consultants, and the future of cloud offerings for small businesses (see sections 5-9).

5 Small Business & Cloud Computing in Context

5.1 Small Business in Australia – A distinctive, limited commercial and technical operating environment

The Australian Bureau of Statistics (ABS) defines a small business as "a business employing less than 20 people" and includes sole proprietorships and partnerships without employees.[1] As at June 2011, small businesses represented 96 percent of businesses in Australia.[2] But simply having fewer people does not mean small business is merely "little big business."[3]

5.1.1 Limited Operating Resources

Small business experiences its own distinct operating environment. In particular, small business suffers from "resource poverty" compared with larger organisations.[4] In terms of cloud computing, this small business resource poverty includes:

- ***limited in-house expertise*** – limited in-house specialist technical and/or legal knowledge necessary to evaluate and capture the benefits of new operational services and technologies. In 2011, almost 90% of Australia's two million small businesses employed less than five people with two-thirds being non-employing entities, eg. sole proprietorships.[5] The corollary is small business' reliance on external social and/or professional networks and consultants to bring in the required skill sets.
- ***limited personnel time*** – a highly time constrained working environment, frequently with personnel working overtime to simply "get the job done" accompanied by occasional, brief periods of downtime to recover.[6]
- ***limited access to finance & inconsistent cash flows*** – limited access to financial resources to finance new projects, and inconsistent, often lumpy cash flows. Small business experiences much higher revenue and profitability volatility. And, with little access to debt or equity financing, small business is often forced to draw on the owner's assets for financing.[7]
- ***limited bargaining power*** – limited bargaining or purchasing power due to the small-scale nature of their business, often exacerbated by a highly fragmented and competitive industry structure.
- ***greater risk tolerance*** – a greater tolerance to risk as a necessary by-product of their commercial and operational environment. Australian small business experience low survival rates – in any one year, more than 15% of all small businesses can be expected to fail; twice the rate of medium- and large-scale businesses.[8] Traditionally, small business has had limited opportunities to conduct small-scale testing of new commercial options, compelling it to place "bigger bets" from time-to-time to remain competitive or grow the business.[9]
- ***short-term management horizon*** – short-term management perspective, frequently the by-product of a highly volatile and competitive market.

5.1.2 An Unsophisticated Technical Environment

> *The technology landscape in smaller organisations and the resources available to tackle Internet malware (malicious software) are likely to be radically different from larger enterprises. However, a security breach is far more likely to have a devastating effect on the revenues or even the survival of a start-up or small business.*[10]

Operating resource limitations, particularly limited in-house technical skills, reflects a distinct technical operating environment for small businesses compared with larger businesses, such as:

- ***Bring-Your-Own-Device (BYOD)*** – in an attempt to save costs while also seeking to boost employee satisfaction, small businesses is likely to have a greater proportion of "Bring-Your-Own-Devices"—permitting personnel to use their own, personal devices on the company network—in the workplace.
- ***mixed business & personal use*** – a by-product of an increased prevalence of BYOD is a greater tendency amongst small business personnel to use their computing devices—laptop computers, tablet devices, mobile phones—for both business and personal use.
- ***greater device sharing*** – for the cash-strapped small businesses it is also likely that device sharing will be more frequent than in larger, more resource-rich companies.
- ***poor software security setup*** – lacking in-house technical expertise, small business are more likely to have poorly setup and poorly maintained firewall, virus protection, and other security software.
- ***irregular software & security updates*** – larger businesses tend to have sophisticated enterprise-wide software systems for the coordinated, regular update and maintenance of software. For the small business—lacking personnel time and/or technical resources—software updates and patches to fix software and security bugs are likely to be more irregular.
- ***poor wireless network security*** – small businesses are avid users of wireless technologies,[11] attracted to its simplicity and flexibility. But a paucity of in-house technical expertise may result in poor wireless network security, rendering the small business vulnerable to network exploitation.
- ***less strict security systems, procedures and policies*** – large corporations typically have restrictive systems and procedures, controlling who can put what software on which devices. Small business does not have the time, human resources, nor technical capabilities for such operating overhead.
- ***latest web browser*** – many larger corporations—with strict software and IT security systems and procedures—are slow to take-up newer web browsers, and are left using Internet Explorer. In comparison, small businesses, largely devoid of such bureaucracy and always on the look-out for new tools, are willing adopters of such new, "alternative" browsers, such as Google Chrome and Firefox.

5.2 What is Cloud Computing?

Cloud computing includes the delivery of computer processing infrastructure (Infrastructure as a Service, IaaS), operating system platforms (Platform as a Service, PaaS) and/or software, databases and storage as a service (Software as a Service, SaaS) on-demand over either a public or private computer network.

However, in practice for small business—and for the purposes of this report—cloud computing means: renting the use of software, databases and storage (SaaS), and possibly operating systems (PaaS) over a public network (such as the internet) without the upfront cost or inconvenience of having to own, install or maintain software and systems.

5.3 Example Cloud Computing Services for Small Business

The range of cloud computing services available to small businesses is vast and growing rapidly. Prominent examples include:

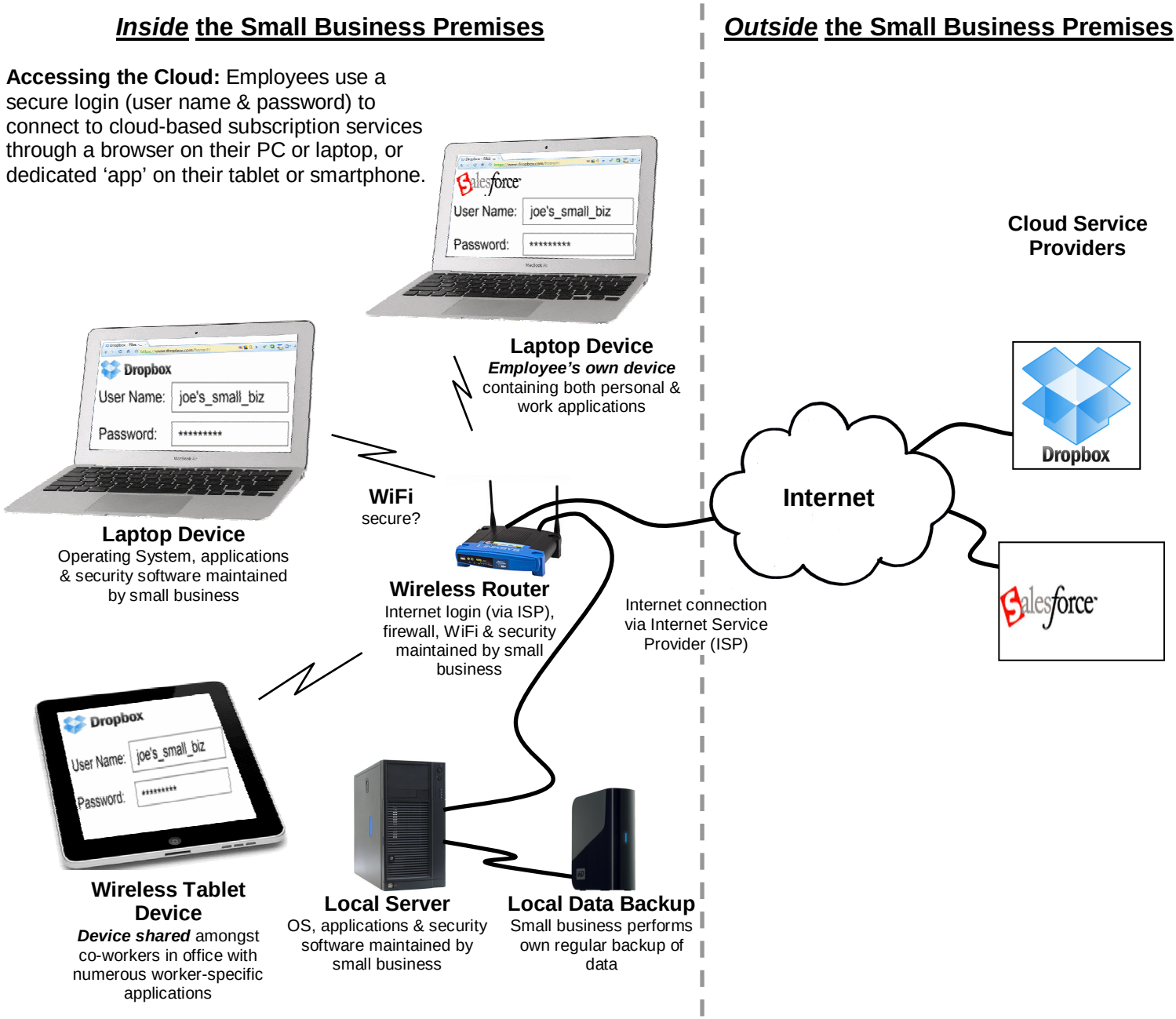
Cloud Service	Provider	Indicative Pricing
Email hosting	Gmail	ad supported
	Hotmail	ad supported
Online data storage	DropBox	free or up to $10+ per month[12]
	Box.net	free or up to $15+ per month[13]
	SugarSync	free or up to $150 per month[14]
Sales force automation services	SalesForce.com	$10+ per user per month[15]
	sugarCRM	$30 - $100 per user per month[16]
	ZoHo CRM	free or up to $25 per user per month[17]
Word processing, spreadsheets, and presentation services	Google Apps	$5 - $10 per seat per month[18]
	ZoHo Docs	$3 - $5 per user per month[19]
Project management	Basecamp	$20 - $150 per month[20]
	TeamGantt	$10 - $79 per month[21]
	Asana	$100 - $800+ per month[22]

Several of the above cloud service providers, such as Dropbox and Box.net, provide a "freemium" subscription services. Under a freemium model, the basic service is provided free of charge, with more advanced accounts with additional functionality attracting subscriptions fees.[23]

5.4 Small Business & Cloud Services: an Example Setup

While cloud computing holds great promises for the small business, as illustrated below, it does not completely absolve the small business of all IT overhead. Small businesses remained tasked with *inter alia*:

- a subscription with an Internet Service Provider (ISP);
- purchase and setup of a modem (ADSL, cable, 3G) to securely connect to the internet via their ISP and, where appropriate, a secure wireless local network);
- purchase and setup of computer(s), printer(s), backup storage, etc.;
- purchase, setup and maintenance of operating system software, security software (eg. firewall, anti-virus, etc.) and other software, eg. web browsers.



5.5 What are the benefits of cloud computing for small business?

> *[Small-to-Medium sized Enterprises (SMEs) do not] have the wherewithal to set up the initial infrastructure that is necessary to realize the cost structures of large data centers. The prices and the [Service Level Agreements] from the leading cloud providers are far better than what most SMEs can realize with their modest investment levels. Even more significantly, cloud computing needs no upfront investment, which will allow cash-strapped SMEs more flexibility with the use of their capital.*[24]

Given the distinct operating constraints of small business—particularly around financial and personnel constraints compared with larger organisations—cloud computing holds out the promise of manifold benefits including:

- ***Financial Benefits*** – smooth, scalable cash flows:
  - *smooth cash flows* – cloud computing obviates the expensive, upfront capital costs of purchasing new computer hardware or software, distributing operational expenses over time. Cloud services are typically paid monthly on a pay-as-you-go (PAYG)/subscription-based basis, spreading and smoothing cash flows over time.
  - *costs scale with the business* – the PAYG model scales up (and down) month-to-month in response to the varying demands of the small business over time. Because of its highly dynamic and scalable nature, cloud computing is well suited to small businesses with their variable and often unpredictable business demand.[25]
- ***Personnel Benefits*** – reduced administrative & personnel overhead:
  - *ease of setup* – cloud computing dramatically reduces IT personnel requirements: cloud services are delivered via a web browser; purchasing and installation involves signing-up to a service through a website, submitting credit card details, and agreeing to the Terms of Service; and training and support needs are often minimal. Combined, cloud computing serves to substantially free-up personnel to do the "real work" for the business, eg. generating sales, developing new products and services, etc.
  - *automatic & frequent service updates* – the small business receives the latest version of the service each time they login or connect to the service; small business personnel are freed from having to install the latest updates, configure the software, transfer data files, etc.
  - *location independent service* – cloud services provides location flexibility for the small business and its personnel, and is frequently cited as a principal reason for adopting cloud services.[26] Cloud services are delivered through a web browser – as long as the user has a reasonable internet connection, the service is the same whether the user is in San Francisco, Sydney or Singleton. Cloud computing means business software, data and communications can be delivered to whoever wants it, whenever they want it, wherever they want it.[27]

- ***Operational Benefits*** – business security and continuity improved:
  - *improved security* – for many small businesses, adopting professional cloud-based services typically represents a significant increase in the secure storage of sensitive information.[28]

    Small businesses may store sensitive information in physical records, rendering them susceptible to misplacement, theft, damage through fire, etc. For digital records, small businesses are unlikely to be experts in computer and network security. They may have poorly setup and/or maintained firewalls and other security software on individual computers and/or network devices, wireless network security may have weak or non-existent security encryption, and local backup storage may not be secured at all.

    In comparison, cloud provider security is developed, monitored and maintained by computer security experts, information is usually stored redundantly over multiple physically separate sites, and service delivery from the cloud vendor to the client's web browser is typically undertaken over a password protected, commercial-grade encrypted internet connection.
  - *increased business continuity* – cloud services replace the need for frequent software installation and updates, and their accompanying service downtime. Cloud services—typically promising 99.9%+ up time[29]—typically represent a significant increase in service availability and business continuity for small businesses.
  - *access a global market* – many small businesses use cloud services to host their business website, sometimes using it as their principal store front, accessing, and promoting their business to, a far larger, potentially global market place.[30]

6 Small Business, Cloud Computing & Cyber Crime

6.1 Computer security risks and criminological issues identified in connection with cloud computing internationally

6.1.1 Computer security and the potential for criminal offences against small business

A number of computer security issues and criminal offences have been identified in the literature that could affect cloud service providers, cloud computing tenants, and the transmission of data between providers and tenants. Many of these vulnerabilities are not unique to cloud computing, but could arise in connection with conventional use of information and communications technologies by small businesses, and, indeed, by larger businesses as well. What is different, however, is the nature of the data that may be stored by businesses on the cloud, and their attractiveness to offenders located in disparate countries. Other vulnerabilities are unique to virtualisation and the multi-tenancy environment of the public cloud.

The impact of computer security incidents arising from cloud computing on small business may be substantial. This may be because small businesses may be directly targeted by cloud computing marketing and advertising agencies, thereby increasing pressure on small businesses to make use of cloud computing services. Also, small business operators are likely to use the devices that connect to their cloud service provider for both personal and work-related reasons creating potential security risks that arise from personal use. Multiple persons may use these devices, thereby increasing the potential for them to be compromised. Due to resource constraints on small businesses and lack of computing expertise, there may be a lack of awareness about computer security risks. Finally, there are no requirements for many small businesses to comply with the data security obligations as set out under the *Privacy Act* 1988. These factors all make the risks for small businesses heightened in the cloud environment.

Compared with computer security incidents affecting corporate systems generally, there have been relatively few attacks reported against cloud service providers.[31] Banham[32] claims that this is because cloud service providers have stronger security as they are more concerned about the consequences of reputational damage if data are breached. According to Pacella,[33] 'cloud providers often ask their clients to keep attacks quiet'. In addition, when not bound by mandatory data breach reporting requirements, as in Australia, cloud computing customers are likely to want to avoid the publicity associated with data breaches. This may be particularly relevant when the cloud service provider claims no responsibility or liability for breaches of data security or un-availability of data in service-level agreements.[34] In addition, some attacks may go undetected, and in other cases when data breaches are made public, the fact that data were held in the cloud may not be released. It is clear that cloud service providers and vendors are reluctant to publicise the insecurity of their systems, and are unwilling to disclose security breaches that occur. Recent survey research has, however, revealed evidence of concern and actual victimisation in connection with cloud computing.

According to an international survey conducted by Trend Micro, an antivirus and computer security vendor, 43 percent of organisations that reported using cloud computing had experienced a "security lapse or issue" in the previous 12 months, although the nature of the incident was not disclosed.[35] Trend Micro surveyed 1,200 companies with over 500 employees in the United States (US), Canada, the United Kingdom, Germany, Japan and India.[36]

Another survey of 103 US and 24 European cloud service providers by the Ponemon Institute revealed that 62 percent were not confident that "the cloud applications and resources they supply are secure."[37] Sixty-five percent of respondents were public cloud providers, while private and hybrid cloud providers each made up 18 percent of the sample. Of the public cloud providers, only 29 percent were confident or very confident that the cloud applications and resources supplied by their organisation were secure.[38]

A survey conducted by a computer security vendor at DefCon, a hacker conference held in Las Vegas, in 2010, found that 96 percent of respondents believed that the "cloud would open up more hacking opportunities for them", and 45 percent had "already tried to exploit vulnerabilities in the cloud."[39] The 100 survey respondents were described as 'IT professionals.'[40]

6.1.2 Attacks targeting cloud service providers

Insufficient or faulty authentication checks

Unauthorised access to cloud computing systems may occur when a username and password combination has been obtained without authorisation. This can occur using a variety of technical and non-technical methods. Social engineering may be targeted towards the cloud service provider by, for example, claiming that urgent access is required but that the password is not working and needs to be reset. Passwords may also be guessed, be left lying around in offices, obtained using keylogging malware, cracked using brute force, or overcome when there are weak password recovery mechanisms,[41] such as answering 'secret' questions where the answers are publicly available. An example of a social engineering attack is provided in Box 1. Social engineering refers to using techniques of influence, deception and persuasion to trick people into disclosing information.

BOX 1

zzzreyes writes "I got an email from my cloud server to reset the admin password, first dismissed it as phishing, but a few emails later I found one from an admin telling me that they had given a person full access to my server and revoked it, but not before 2 domains were moved from my account. I logged into my account to review the activity and found the form the perpetrator had submitted for appointment of new primary contact and it infuriated me, given the grave omissions. I wrote a letter to the company hoping for them to rectify the harm and they offered me half month of hosting, in a sign of good faith. For weeks I've been struggling with this and figure that the best thing to do is to ask my community for advice and help, so my dear slashdotters please share with me if you have any experience with this or know of anyone that has gone through this. What can I do?"

Source: http://it.slashdot.org/story/12/04/04/1738220/ask-slashdot-my-host-gave-a-stranger-access-to-my-cloud-server-what-can-i-do?utm_source=rss1.0moreanon&utm_medium=feed

The following incident allegedly involved weak password security, although the specific vulnerability was not disclosed:

> *In a recent high-profile security breach, a hacker took advantage of the weak password security of a cloud service provider to hijack a Twitter employee's email account, giving him access to personal and corporate documents at Twitter.*[42]

However, insufficient or faulty authentication checks may not necessarily be attributed to malicious activity, although it may result in data being accessed for nefarious purposes. For example, the following incidents allowing others to access data stored on the cloud were described as being 'inadvertent' or a 'mistake':

> *In June 2011, Dropbox, a popular cloud storage site where approximately 25 million people store their videos, photos, documents, and other files, inadvertently left the site open for four hours on Father's Day. The glitch let anyone log in to customers' accounts with any password.*[43]

> *In March, Google itself made a mistake in Docs' sharing feature that enabled users who were collaborating on one document to access others.*[44]

> *The Microsoft Business Productivity Online Suite, aimed at commercial enterprises, reportedly was hit with a data breach in 2010, and customers of the BPOS cloud services apparently could download information on other customers of the suite, albeit inadvertently.*[45]

Insufficient or faulty authentication checks may also provide opportunities for Uniform Resource Locator (URL) guessing attacks, whereby possible page links are entered to access pages directly, bypassing authentication checks.[46]

Data breaches, however they are accomplished, may have significant impacts not only on the cloud service provider's tenant whose data have been accessed, but also on customers who may have trusted that organisation with their personal information:

> *In early April, Epsilon announced that its database had been breached by an unknown third party, allowing unauthorised access to the email addresses of its clients' customers.*[47]

In other instances, it may be the cloud service providers' records that are compromised:

> *Other commercial [cloud service providers] have suffered breaches, such as GoGrid, which reported last March that an unauthorized third party possibly had viewed its customers' account information, including payment card data.*[48]

> *In November 2007, Salesforce.com, a web-based [customer relationship management] service provider, warned its customers that they might be the targets of some phishing scams after one if its employees was tricked into divulging a corporate password. With the obtained password, the perpetrators were able to access names, e-mail addresses, and telephone numbers of Salesforce's customers, and they sent out fake invoices.*[49]

Denial of service attacks

Denial of service (DoS) attacks against cloud service providers may leave their customers without access to their accounts.[50] This can occur by sending a flood of traffic to overwhelm websites to make them inaccessible to legitimate users. When a DoS attack is conducted using a botnet, a network of compromised machines, this is referred to as a distributed denial of service attack, or DDoS.

DoS attacks aimed at individual accounts, rather than to all cloud tenants, may also be accomplished by changing the tenant's password or maliciously continuing to enter the incorrect password so that the account becomes locked.

Use of cloud computing for criminal activity

Cloud computing accounts can be created or existing accounts compromised for criminal purposes. New cloud computing accounts may be created with stolen credentials and credit card details, thereby reducing the cost to the offender(s), as well as anonymising the offender and creating further difficulties in tracing down the source of the attack, particularly when jurisdictions are crossed. Accounts created or compromised in such a way can be controlled as part of a botnet.[51] In the following example, an existing cloud computing account was compromised and used to run a botnet command and control server:

> *ComputerWorldUK reported in December 2009 that a website hosted on Amazon EC2 had been hacked to run the Zeus botnet's command-and-control infrastructure.*[52]

Botnet command and control servers can be used to launch denial of service attacks, conduct scams such as click fraud, and distribute spam.[53] The processing power of botnets may also be used to conduct brute force attacks to overcome password restrictions.[54] This is potentially what happened in the following case:

> *There have also been reports that hackers were suspected to have made use of the cloud computing server of* [a technology corporation] *to launch attacks on the payment platforms for online games and entertainment services of a well-known Japanese technology corporation and its subsidiaries in April this year, causing leakage of the personal data (including name, date of birth and email address) of nearly a hundred million users across the globe, and it was believed that the data of over 11 million credit cards had probably been leaked.*[55].

Cloud computing services may be used for the storage, distribution and mining of criminal data such as stolen personal information or child exploitation material.[56] Accounting systems run in the cloud may be attractive for money laundering and terrorism financing activities.

The use of cloud computing to conduct illegal activities has had further negative consequences in relation to data access for the other, legitimate, users of the cloud service provider when servers have been seized by a law enforcement agency.[57] Not only may access be disrupted, but the law enforcement agency, international or domestic, may have access to that data in a multi-tenanted environment.[58]

Illegal activity conducted by cloud service providers

Loss of access to data has also occurred when the cloud service providers themselves are allegedly engaged in other illegal behaviours. In the following example the cloud service provider's services were stopped due to police action:

> *January's big local technology story was the police raid of Kim Dotcom's Coatesville mansion. Dotcom and his colleagues were arrested because of allegations the Megaupload cloud storage service he ran was a piracy operation. There is no doubt some people used the service to swap movies and music files. Yet Megaupload was also a low-cost way of legitimately sharing files and a cheap place for making online backups. It was a basic*

cloud storage facility. Megaupload's legitimate business didn't stop the US authorities shutting the service without warning. Sudden closure left businesses unable to access their documents.[59]

Attacks on physical security

The cloud service provider's data centre may be physically attacked, resulting in hardware theft, unauthorised access to servers or loss of access to data.[60] Data centres such as those used by cloud service providers have reportedly had their physical security breached:

In a style reminiscent of the 'wild west' days of the nineteenth-century United States, two masked men allegedly pistol-whipped a lone IT staff worker during a graveyard shift, held the worker hostage for 2 h while confiscating equipment in a Chicago data centre. The burglars reportedly entered the facility through a fire escape and passed an unoccupied security guard post. The thieves waited in hiding for the IT staffer to leave the data centre and then ambushed and subdued the victim. The thieves swiped the staffer's access card through a reader and forced him to perform a finger print scan before stealing computer storage equipment.[61]

Insider abuse of access

Cloud service provider insiders, such as employees, contractors or third party suppliers, may misuse their privileges and disrupt access or obtain unauthorised access to stored data.[62] Insiders may obtain employment at a targeted cloud service provider, be targeted by organised crime syndicates, abuse their access as the result of becoming discontent in their employment, or become tempted by presented opportunities and the potential perceived gains.

Compounding this issue is that data may not be deleted adequately by the cloud service provider, particularly when data has been replicated over several locations to maintain availability or services have concluded.[63] This creates further opportunities for these data to be later accessed or misused.

Malware

The cloud service providers' servers may be vulnerable to malware infection, including virtual machine based rootkits.[64] These risks apply in non-cloud environments as well. Malware infection end may result in account names and passwords being compromised, files being accessed and copied, corruption of files or being added to a botnet, a network of compromised machines. There is also the possibility that malware compromising one tenant's virtual machines could then spread to the virtual machines of other tenants.

Side channel attacks or cross-guest virtual machine breaches

"Side channel attacks", or "cross-guest virtual machine breaches" may result in tenants crossing the shared virtual machine boundaries and accessing the data of other tenants using shared physical resources.[65]

Side channel attacks require the attacker's virtual machine and victim's virtual machine to be located on the same physical machine; therefore these attacks may be random, and not targeted towards a specific tenant. However, targeted attacks may still be possible. It has been demonstrated with one cloud computing service provider that co-tenancy could be successfully achieved 40 percent of the time by setting up

new accounts while simultaneously manipulating the resource needs of the targeted victim's virtual machines.[66]

Vulnerabilities in software applications

Security holes and vulnerabilities may exist in software applications run in the cloud, such as backdoors that bypass normal authentication protocols.[67] New vulnerabilities for operating systems, internet browsers and business applications are regularly being identified. Security patches fix vulnerabilities in computer programs that may be used to gain unauthorised access. However, delays in installing patches may lead to increased exploitation attempts as the vulnerabilities they are fixing are then made known.[68]

Similarly, insecure application programming interfaces, which allow software applications to interoperate with each other by passing login information between them, may provide another attack vector.[69] Application programming interfaces may be used, for example, to share data across different applications, which requires the transmission of authentication tokens from one application to the other.

Web browsers, used to access the internet and cloud service providers, are a type of software application. Browser vulnerabilities have reportedly been exploited to gain access to data stored in the cloud:

> *Google on Tuesday said that in mid-December it faced "a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google". Attackers were apparently attempting to access the Gmail accounts of Chinese human rights activists, and also launched attacks against more than 30 other companies. Later in the week, it was reported that a flaw in Internet Explorer had been exploited to hack into Google's corporate networks, and Microsoft said it was working on a patch.*[70]

Browser vulnerabilities include cross site scripting, whereby code is injected into websites and executed by the browser.[71] Cross site scripting can be used to hijack sessions by obtaining cookies (refer to attacks targeting the transmission of data below) or obtain authentication credentials by redirecting users to a site impersonating the cloud service provider.

Cryptanalysis

Data stored in the cloud may be encrypted to prevent it from being read if accessed without authorisation. However, encryption can potentially be weakened or broken if insecure or obsolete.[72] Partial information can also be obtained from encrypted data by monitoring clients' query access patterns and analysing accessed positions.[73]

SQL injection

Structured Query Language (SQL) is a programming language used for database management systems. SQL injection attacks targeting web entry forms involve inputting SQL code that is erroneously executed in the database back end.[74] SQL injection attacks can result in data being accessed and modified without authorisation. Another injection attack is OS injection[75] or command injection,[76] whereby the input contains commands that are erroneously executed by the operating system.

6.1.3 Attacks targeting cloud computing tenants

Phishing

Although, in the context of cloud computing, phishing misrepresents the provider, the attack is directed towards those who may hold an account with that organisation, with the aim of obtaining passwords and other identifying information to obtain unauthorised access to data held in the cloud.[77] Phishing is one example of social engineering, in which an email appearing to be from a legitimate organisation is sent directing recipients to a bogus (spoofed) website to enter their login credentials or other personal information. Salesforce was reportedly misrepresented in a phishing attack in 2007[78] and Google's Gmail in 2009.[79]

Although phishing often involves random attacks, whereby emails are sent out to en mass, individuals within organisations may be directly targeted, known as spear phishing. In spear phishing, the attack is tailored to enhance its perceived legitimacy, such as appearing to come from a service provider that the business deals with.[80]

Domain name system attacks

Cloud computing users may be subject to domain name system (DNS) attacks.[81] The principal use of domain names is to convert an internet protocol resource, a string of numbers, into a readily identifiable and memorable address, such as those used in email addresses and URLs. The following types of DNS attacks are aimed at obtaining authentication credentials from internet users, including cloud service tenants:

- pharming and DNS-poisoning (diverting visitors to spoofed websites by 'poisoning' the DNS server or the DNS cache on the user's computer);
- domain hijacking (stealing a cloud service provider's domain name) or domain sniping (registering an elapsed domain name);
- registering a domain name that appears to be similar to a cloud service provider (cybersquatting) in order to conduct phishing scams, or to obtain login details by typesquatting, which relies on a user entering the wrong URL and subsequently providing their authentication credentials to a spoofed website.

Compromising the device accessing the cloud

Access to a business's cloud computing account may be achieved if the device that is accessing the cloud services is compromised, for example, by a keylogger that records keystrokes, including usernames and passwords.[82] Again, malware infections such as this may be random, or individuals within an organisation may be directly targeted with a Trojan, malware designed to look like a legitimate file.

Access management

Businesses that fail to restrict their employees' access to cloud computing services after they leave their employment would be vulnerable to having their data accessed, altered, copied, or deleted.[83] Former employees may seek revenge against their employer, or steal information for resale or to use in setting up a competing business. Such risks, of course, also exists in the non-cloud computing environment.

6.1.4 Attacks targeting the transmission of data

Session hijacking and session riding

Session hijacking involves the attacker exploiting active computer sessions by obtaining the cookies that are used to authenticate users.[84] As discussed in relation to browser vulnerabilities, one way that this can be achieved is cross site scripting, which involves malicious code being injected into the website, which is subsequently executed by the browser.[85]

A similar attack is called session riding, in which websites are exploited using cross site request forgery to transmit unauthorised commands.[86] An attacker 'rides' an active computer session by tricking a user, for example, by sending a link, to visit a manipulated webpage while they are logged into the targeted site. The webpage contains a request which is executed by the website as the user is also sending their authentication credentials. Commands may be used to, for example, manipulate or delete data, reset passwords, add new users or delete existing users, or forward emails.[87]

Man-in-the-middle attacks

In a man-in-the-middle attack the attacker intercepts traffic between a website and a browser.[88] This occurs when the browser believes that the attacker is the legitimate website, and the website authenticates the attacker as the browser. The attacker can then read and alter the data being transmitted, including account passwords that may be used to login to cloud services.

Network/packet sniffing

Network or packet sniffing involves the interception and monitoring of network traffic.[89] Data that are being transmitted across a network, such as passwords, can therefore be captured, and read if not adequately encrypted. In the cloud environment, this is particularly important as passwords play a critical role in establishing access to the provider's services.

6.2 Potential for small business to commit offences

6.2.1 Using the cloud to commit offences

As indicated above, the cloud may be used to commit offences such as launching denial of service attacks, conducting scams, distributing spam, conducting brute force attacks and the storage, distribution and mining of stolen personal information and child exploitation material. However, there is the potential for businesses to misuse the cloud in other ways. For example, businesses may find that they have breached copyright legislation if files are made available on the cloud for distribution to others. There is also a potential for businesses to hide records in offshore cloud services in an attempt to avoid privacy or taxation requirements.

6.2.2 Failure to report serious offences

Despite a recommendation by the Australian Law Reform Commission (ALRC) in 2008,[90] there is currently no requirement in Australia for businesses to advise individuals if their personal identifying information has been breached accidently or as the result of unauthorised access to a computer system. However, section 316(1) of the New South Wales *Crimes Act* 1900 may be applicable when a business owner does not report that data has been compromised to a law enforcement agency:[91]

> *If a person has committed a serious indictable offence and another person who knows or believes that the offence has been committed and that he or she has information which might be of material assistance in securing the apprehension of the offender or the prosecution or conviction of the offender for it fails without reasonable excuse to bring that information to the attention of a member of the Police Force or other appropriate authority, that other person is liable to imprisonment for 2 years.*

A serious indictable offence is defined as an indictable offence that is punishable by imprisonment for life or for a term of 5 years or more. Serious computer offences in New South Wales include:

- s.308C Unauthorised access, modification or impairment with intent to commit serious indictable offence;
- s.308D Unauthorised modification of data with intent to cause impairment; and
- s.308E Unauthorised impairment of electronic communication.

Similar provisions do not exist in other Australian jurisdictions, except where a benefit is obtained in exchange for not reporting.[92]

There are a number of reasons why businesses may not report computer security incidents. The AIC's ABACUS survey of Australian businesses revealed that in the 2006/07 financial year, 77 per cent of respondents that had experienced a computer security incident dealt with their most serious incident internally; eight per cent reported the incident to the police, three per cent reported to a non-police enforcement or regulatory agency, and 11 per cent reported to another organisation such as Visa or MasterCard, a lawyer or AusCERT.[93] In 2006 AusCERT's Australian Computer Crime and Security Survey found that of the respondent companies that had experienced any type of electronic attack, 69 per cent chose not to report it to anyone outside their organisation.[94] Reasons for not reporting included, among others: perceived negative publicity (46 per cent); not being aware of law enforcement interest (52 per cent); not thinking perpetrators would be caught (57 per cent); and not thinking law enforcement was capable (55 per cent).[95]

6.3 Computer security risks and criminological issues likely to arise over the next two years

The popularity of cloud computing services coincides with other technological developments and associated threat vectors. Potential security risks relating to cloud computing that are likely to arise in the near future include security risks relating to mobile computing, issues relating to employees bringing their own devices to the workplace, and attacks exploiting new vulnerabilities, including those that have been designed to improve security.

6.3.1 Mobile and wireless computing

Coinciding with the improved portability of computers, such as laptops, smartphones, tablets and other devices, is the increased accessibility of the internet through wireless internet connections. Business owners therefore can connect to the cloud service provider where Wi-Fi networks are provided, such as airports, cafés, restaurants, libraries or hotels, or use internet connections that have inadvertently (or maliciously) been left open. Users of unsecured Wi-Fi connections, or connections that are protected with weak encryption, are at risk of having their sessions hijacked, leaving

their accounts accessible to other network users without their knowledge. This occurs when the cookies, used to authenticate the user, sent by an unencrypted website, are intercepted and used to impersonate the account holder.[96] An attacker may also create a Wi-Fi access point that impersonates a nearby business to use in a man-in-the-middle attack, intercepting the traffic between a website and a browser.[97]

6.3.2 Employees bringing their own devices

Corporations are currently struggling with how to manage employees bringing their own devices (BYOD) to the workplace. These may include smartphones, laptops and tablet computers, as well as peripherals such as USB flash drives, which can be used to transmit malware. The benefits of BYOD include fewer costs to the business in providing computers, as well as reportedly improved employee satisfaction. However, there are also concerns about the security, particularly when employee-owned devices are not managed by the business and therefore may not be appropriately patched or have anti-virus installed.[98] Also, devices that are used for personal computing may be susceptible to malware such as trojans disguised as games and there are an increasing number of reports of malicious applications designed to collect sensitive data from smartphones.[99] The use of compromised BYOD devices to access cloud services may create more avenues for unauthorised access.

6.3.3 Manipulation of costs

Due to the cost model of cloud computing, with users typically paying for the amount of resources they consume, there exists an opportunity for business competitors to increase the costs for a targeted business by increasing their data demands. Such attacks would be similar to the reports of denial of service attacks conducted in order to diminish competitors' market presence,[100] however this attack would be aimed at increasing a business's expenditure rather reducing its revenue.

6.3.4 Attacks exploiting new vulnerabilities

The market for newly discovered computer security vulnerabilities, known as zero-day exploits, is reportedly lucrative,[101] and technologies developed to deflect offenders may actually be of practical use to facilitate criminal behaviour. As a result, there continues to be a technological battle at play between offenders and those that are concerned with securing systems and information. For example, RSA announced in 2011 that it had been targeted in an attack that included obtaining information relating to RSA's SecurID two-factor identification products.[102] The SecurID tokens display an authentication code which provides access to a computer system when used with a password or personal identification number. RSA later replaced RSA tokens after Lockheed Martin, one of their clients, reported that they had been targeted in an attack.[103] As ways to verify one's identity become more sophisticated, the implications for compromises increase. For example, compromised biometric data, such as fingerprints or voiceprints, are not as easy to replace as a password or identity token.[104]

6.4 Computer security and criminological issues particularly affecting small business

Although most of the risks identified above apply to all business sizes, others have specific concerns for small business. The Australian Bureau of Statistics' definition of small business was adopted for this research, which is a business with fewer than 20

employees.[105] Small businesses therefore may not have in-house information technology expertise and hence see cloud computing is an attractive alternative.

6.4.1 Marketing towards small business

Cloud service providers may specifically market small businesses, touting the economies of scale and other potential benefits as to why they should take up software-as-a-service or platform-as-a-service.[106] As 96 percent of businesses in Australia are small businesses,[107] cloud service providers are likely to market their products directly to this demographic. However, marketing and advertising may be deceptive or not disclose the full extent of crime risks and liability issues. Furthermore, the benefits touted to small businesses may not necessarily be evaluated or realised by all.

6.4.2 Combined personal and business computer use

When business computers are also used for personal purposes there are additional challenges in relation to opportunities for the device to be compromised. When a small business is operating from a home office there may also be a higher chance that multiple people would use the one computer. This issue is related to employees bringing their own devices into the workplace as discussed in the previous section.

6.4.3 Lack of awareness about security risks

Computer security may not be a high priority for small business owners. This may be because they are not necessarily aware of the security risks involved in cloud computing, how they may relate to them, and the possible outcomes of a computer security incident, such as loss of access to data and reputational damage. As 64 percent of small businesses are sole operators,[108] they may lack specific expertise in information technology, specifically computer security. Businesses may not understand what they are responsible for under a cloud service provider's service level agreement (SLA). Also, while cloud service providers may market their products as being more secure, businesses may not be aware of the greater avenues for attack afforded by having their data stored in the cloud. This may be particularly relevant for attacks targeting the cloud computing tenant, such as compromising their computer with malware or phishing attacks.

6.4.4 No obligations under the *Privacy Act 1988*

The *Privacy Act* 1988 (Cth) (the Privacy Act) sets out ten National Privacy Principles (NPPs), relating to personal information. The NPPs relate to data collection, use and disclosure, data quality, data security, openness, access and collection, identifiers, anonymity, transborder data flows and sensitive information. However, small businesses are currently not required to comply with the NPPs as set out under the Privacy Act unless they:

- have an annual turnover of more than $3 million;
- are health service providers;
- contract to Australian Government agencies;
- are legally related to an organisation covered by the Act;
- disclose personal information for a benefit, service or advantage; or

- provide someone else with a benefit, service or advantage to collect personal information.[109]

The lack of obligations under the Privacy Act could lead to inappropriate handling of personal information. The ALRC recommended in 2008 that the small business exemption be removed.[110] However, the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 currently before parliament does not remove the small business exemption.

6.4.5 Severity of impact on small business

Small businesses may also not have the means to recover financially from disruptions caused by loss of access to data. Small businesses may be particularly vulnerable to changes in income and expenditure. For example, of businesses registered in 2007/09, only 43 percent of businesses conducted by sole operators were still operating in 2011, compared with 60 percent of employing businesses.[111]

6.5 How threats are being addressed by small businesses and cloud computing providers

Many of the prevention measures that can be adopted by small businesses that are outlined below to prevent computer security incidents are general in nature, rather than unique to cloud computing environments. However, some of the prevention measures that may be implemented by cloud service providers, such as physical security of data warehouses, take the onus away from the small business. Therefore, it would be expected that the physical security of cloud service providers would be greater than what could be afforded by the small business owner who might otherwise be running a server from an unsecured location that can be accessed by others. This section also discusses the possibility of crime displacement as the result of prevention measures.

6.5.1 Technical prevention measures

Technical prevention measures can be adopted by both the small business and the cloud service provider. Technical prevention methods include:

- patching operating systems, internet browsers and other software applications to protect against new vulnerabilities and malware;[112]
- installing anti-virus and malware tools;[113]
- installing firewalls to protect against unauthorised access;[114]
- using multifactor authentication to strengthen authentication checks;[115] and
- encrypting data travelling between the cloud and the browser, as well as encrypting data stored in the cloud[116] to protect against attacks targeting the transmission of data, as well as limiting the effects of unauthorised access.

Cloud service providers may also use intrusion detection and prevention systems and network monitoring.[117]

6.5.2 Physical security

Cloud service providers should be providing a safe and secure data warehouse that can only be accessed by authorised personnel in order to prevent attacks against

physical infrastructure as well as insider abuse of access. Physical security measures include:

- perimeter security, such as bunkers, gates and fences;[118]
- shielded server rooms and cages that prevent eavesdropping, external scanning and interference via electromagnetic radiation;[119]
- surveillance, such as CCTV and security guards;[120]
- access control, such as swipe cards, turnstiles, biometric authentication and identity cards;[121] and
- maintaining facility access logs.[122]

Cloud service providers should also have effective fire management practices in place and backup power systems to prevent data loss through natural disaster or malicious attacks.[123]

While security audits should assess whether appropriate physical security measures are in place, as discussed in the following section, audit rights may be beyond the scope of small businesses.

6.5.3 Organisational policies, awareness and training

Small businesses may implement a number of organisational policies to protect against computer security threats that relate to cloud computing, as well as computer security more generally, including:

- IT-acceptable use policies that set out how a business's computer resources should be used, including expectations in relation to personal use, the handling of sensitive information, the installation of applications and the forwarding of emails, which may contain malware;[124]
- password policies that set out how often passwords should be changed and their complexity to strengthen authentication checks;[125]
- user access management policies that set out the access rights for staff, including that access should also be discontinued when a staff member leaves an organisation;[126]
- policies relating to employees using their own devices into the workplace, which may be vulnerable to compromise and create more avenues for unauthorised access to cloud services.[127]

Small businesses may also provide training to staff and create awareness about computer security issues.[128] Ensuring staff are well informed may assist in preventing social engineering attacks such as phishing that are not necessarily protected against by technical measures.

Because of the sensitive nature of data stored by cloud service providers, they should also conduct background checks when employing staff as a preventative measure against insider abuse of access.[129]

The AIC's ABACUS survey of Australian businesses revealed that small business respondents were less likely than medium and large businesses to have staff policies or training in place. Only seven percent had IT-acceptable use policies, 19 percent had account/password management policies, 12 percent had user access management policies, and 15 percent provided employee education and awareness programs.[130]

6.5.4 Service level agreements

Small businesses should be aware of the implications of their cloud service provider's SLA, which will address the issues of security, privacy and data control.[131] SLAs may also set out requirements for third party audits of cloud service providers.[132]

6.5.5 Crime displacement risks

Crime displacement occurs when crime moves to other locations, times, targets, methods, perpetrators, or types of offence, often as the result of crime prevention initiatives.[133]Displacement concerns that relate to cloud computing may include:[134]

- displacement to cloud service providers that do not have strong security measures;
- displacement to cloud service providers operating from jurisdictions that do not have applicable criminal provisions, have low criminal penalties, or do not have extradition treaties;
- displacement to different methods, for example, if a target is adequately protected against electronic attacks, an offender may coerce an employee through bribery or extortion; and
- displacement to perpetrators who are more highly skilled and perhaps more adept at hiding their offending activities.

Effective crime prevention requires an appreciation of these risks and the use of measures designed to address them.

7 Small Business, Cloud Computing & Regulatory Compliance – The potential for small business to commit offences

7.1 Regulatory Compliance – The obligation of small business

> *If you are in business and fail to meet government regulations it will be you and not your cloud storage provider who will face fines and/or imprisonment.*[135]

With limited personnel, small business has the onerous challenge of keeping up to date with an ever changing sea of regulations and their practical implications. The introduction of cloud services compounds the problem further.

Regulatory compliance remains the responsibility and obligation of the user of the cloud services—ie. the small business—not its cloud service provider.[136]

Assuming small business is aware of and understands the relevant regulations, the small business—with its inherent operating constraints, including financial, personnel, technical and legal—must now also undertake ongoing evaluation of their own cloud service providers' offerings vis-a-vis those regulations.

Furthermore, ever cost-conscious small businesses are more likely to favour lower-end, budget cloud solutions that are unlikely to be tailored to meet regulatory requirements from time-to-time. Accordingly, small business "will likely also need to develop a reasonable plan for migrating off the cloud computing platform if necessary to comply with changes in laws that are not addressed by the provider's offering."[137]

7.2 Audit Rights – A potential big problem with no solution for small business

Audit rights are fundamental to ensuring regulatory compliance. But for cloud service providers, audits represent potentially significant disruption. For example, basic security audits involve at a minimum physical inspection of facilities and access procedures.[138] Accordingly, only the largest organisations are likely to receive adequate audit rights, largely leaving small business out in the cold.[139]

To minimize disruption and placate concerns, some cloud service providers have secured specific audit approval (eg. SAS70 Type II). But such service provider-contracted audits are typically only available to clients under a non-disclosure agreement,[140] unlikely to be accessible to small businesses. More fundamentally, being service provider-contracted audits and not independent, they may be insufficient for regulators.[141]

Irrespective of who undertakes the audit, there remains uncertainty—even amongst larger organisations—as to what a sufficient audit looks like:

> *… while most user companies recognise the value of being able to audit cloud computing; they, too, have little understanding of what should be audited.*[142]

If what should be audited is potentially beyond the scope of large-scale enterprises, how can small businesses be expected to cope?

7.3 Privacy & Data Security – Regulatory molasses for small business

Security and privacy are typically among the principal concerns for all potential cloud computing users.[143] Data integrity, privacy and security issues may be enforced via regulatory or contractual obligations.[144] The exact nature of the regulatory obligations may vary by industry, geography and the practices of the business.

For small businesses with limited personnel time, wading through the multiple layers of international, national and (potentially) state-level regulations and/or standards goes beyond comprehension to the point where most simply give up, prepared to play a game of commercial Russian roulette.

Overarching Regulations

Irrespective of the industry, a business using cloud services will often be subject to multiple, overlapping and overarching regulations. This is particularly the case regarding the management and protection of personally identifiable information. For example, an Australian-domiciled small business selling goods and/or services into (for example) Boston, Massachusetts in the United States may be subject to regulations at the Australian state and/or national level, and also at the United States state and/or national level.

- ***Australian Regulation*** – the collection, use and disclosure, security, accuracy, storage, and overseas transmission of "personal information," including information stored in the cloud, is regulated by the *Privacy Act* 1988 (Cth) and its ten National Privacy Principles.[145] Under the *Act*, "personal information" is broadly defined as:

  > *... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*[146]

  Importantly, "small business"—defined as a business with turnover of $3 million or less in the previous financial year[147]—is substantially freed of the Act's regulations.[148] For many small businesses, therefore, this aspect of the *Privacy Act* is of little concern.

  Health, Genetic & Other 'Sensitive' Information – However, all businesses irrespective of turnover are regulated by the additional protections afforded to "sensitive information" which includes information about racial or ethnic origin, political opinions, sexual preferences, and health and genetic information.[149]

  Security – Under Principle 4.1, *National Privacy Principles, Privacy Act* imposes requirements:

  > *… an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.*[150]

  The Guidelines to the National Privacy Principles provides "tips for compliance" including a "risk assessment – identifying the security risks to personal information held by the organisation and the consequences of a breach of security."[151] Can a small business, with widely varying technical

skills and limited personnel time, adequately undertake such a risk assessment? The answer is: rarely, if ever.

As highlighted in the Truman Hoyle White Paper: "Cloud service providers can assist customers to perform the appropriate risk assessments by being open about the security regimes they have in place … and by contractually committing to specified levels of security."[152] Unfortunately, cloud service providers typically fail to be open and/or provide minimal (if any) such contractual commitments.[153]

In practical terms for small business, cloud service providers are often "in a position to offer very sophisticated approaches to security beyond the capability of many individual businesses."[154] Unfortunately, their ability to increase security in practical terms is rarely matched by a capacity to demonstrate increased regulatory compliance.

- ***United States Federal Regulation*** – If a small business delivers goods or services into the United States (for example), it must comply with the US *Federal Trade Commission Act* (FTC Act) prohibiting unfair and deceptive acts or practices.[155] For businesses storing information in the cloud, this prohibition is likely to extend to the accuracy of a business' privacy policies for collecting, storing and using private information in the cloud, and whether the business—via its cloud service provider—has implemented "reasonable" and "appropriate" controls to secure sensitive personal information.[156]

  The *Fair and Accurate Credit Transaction Act* (FACTA)[157] also applies to any firm that provides products and services and a bill for payment in the United States.[158] FACTA requires such businesses in possession of consumer information must properly dispose of the information. Under FACTA, the Red Flags Rule requires businesses to develop and implement an identity theft prevention program.[159]

- ***State Regulation*** – In addition to national-level regulation, businesses may also be regulated by individual state laws and regulations. For example, the state of Massachusetts has its own regulations safeguarding Massachusetts residents' personal information.[160] Nevada has similar regulatory requirements.[161]

For a larger organisation with sufficient resources, identifying, monitoring and maintaining such compliance may be achievable. But given the potential burden on the organisation, for the cash-strapped, time-poor small business opportunistically looking for every sale possible, achieving compliance as illustrated above would seem wholly unrealistic.

7.4 Document Retention & Maintaining Records

A wide range of Australian state and federal laws require businesses maintain various financial, employee and other business-related records. Small businesses—seeking to save costs wherever possible—may rely almost exclusively on the cloud to store such records. In the event of a service outage, small businesses therefore run the risk of non-compliance.

Legislation Requiring Business Maintain Records – The *Corporations Act* 2001 (Cth) requires financial records be kept for seven years.[162] Similarly, the *Fair Work Act* 2009 (Cth) requires businesses to maintain records of employee information (such as time and wages) for seven years. Under the *Income Tax Assessment Act* 1936

(Cth), businesses must keep records of income tax, Goods and Services Tax, payments to employees and other business payments for five years.[163] The *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (Cth) requires "reporting entities"—primarily the financial and gambling sector (including internet and electronic gaming service providers)—must maintain records of "information relating to the provision of a designated service" (such as electronic funds transfers) for seven years.[164]

Similar laws exist at the state-level. The *Work Health and Safety Act* 2011 (NSW) requires businesses maintain records of all serious workplace health and safety issues for at least five years. The *Industrial Relations Act* 1991 (NSW) requires employees' timesheets be maintained for at least six years. Some industry-specific codes of practice are mandatory. For example, under the *Motor Dealers Act* 1974 (NSW), motor dealers are required to maintain a register of all motor vehicles that they have acquired and/or disposed of.

Despite being a complex soup of overlapping requirements, these are all standard regulatory requirements for businesses; nothing unusual. But combine them with cloud-based storage—which stores records electronically and (potentially) internationally—and things start to get complicated (and challenging) for small businesses.

Storing Records Electronically – To comply with Australian tax laws, businesses that keep records electronically must be able to show that the computer system is safe and accurate, including having:[165]

- control over access to the computer, for example, through the use of passwords;
- control over incoming and outgoing information;
- control over processing of information; and
- back-up copies of computer files and programs and the ability to recover records if the computer system fails.

The person maintaining the system "should have an understanding of [the] computer system," and "[s]ystem documents should be retained to explain the basic aspects of the system."[166]

In addition, records should be kept including "a chronological record and explanation of all changes and upgrades to the software and hardware employed in the system."[167] Does this extend to upgrades to the software and hardware of cloud service providers? If so, this is almost certainly beyond the scope of substantially all cloud customers, but particularly small businesses struggling simply to survive.

Storing Financial Records Overseas – If a business intends to store financial records overseas, it must inform the Australian Securities and Investment Commission (ASIC) "in the prescribed form" of where the information is to be kept.[168] But exactly where data is stored in the cloud varies from over time – particularly among the lower-end, "freemium" cloud offerings popular among small businesses. And while larger organisations with stronger bargaining power may be able to demand their data be stored in a particular fixed geography, small businesses cannot. Often the small business may be wholly unaware its files are being stored overseas (eg. using Dropbox to store a business' MYOB accounting files[169]), and therefore unaware of the need for prescribed notice. How then can a small business—attracted to the cost,

administrative and other benefits of the cloud—hope to comply with the regulatory requirements of the *Corporations Act*?

7.5 Industry-Specific Regulations

Depending on the nature of the business, in addition to overarching regulations, the business may also be subject to industry-specific regulations and/or industry standards requirements. For example:

Financial Services – Financial institutions in Australia are regulated by the Australian Prudential Regulation Authority (APRA). A regulated entity must consult APRA prior to entering an offshore agreement involving a material business activity[170] which may include email, calendar and CRM solutions (eg. Salesforce) hosted in the cloud.[171]

Similarly, businesses looking to deliver financial products and/or services into the United States must comply with the *Gramm-Leach-Bliley Act*[172] (GLB Act) and related legislation.[173] GLB Act compliance is mandatory, and requires businesses to make certain disclosures in an initial and subsequent annual privacy statement to customers. The collection, disclosure and protection of customer information must also comply with the GLB Act's three principal provisions:[174]

- *Financial Privacy Rule* – financial institutions must give customers privacy notices explaining the firms information collection and sharing practices, and provides the customer with the right to limit information sharing;
- *Safety Rule* – all financial institutions design, implement and maintain safeguards to protect the confidentiality and privacy of personal consumer information; and
- *Pretexting Protection* – provisions ensuring the protection of consumers from individuals and companies that obtain their personal information under false pretenses.[175]

Online Payment Compliance & the Payment Card Industry Data Security Standard (PCI DSS) – A small business will commonly use their websites not only to generate leads, but to act as a storefront, enabling customers to purchase goods and services through its website using (for example) credit cards.[176] If the small business manages card payments itself (ie. collecting card name and number details), the small business will typically have a contractual relationship with each of the various card payments companies (eg. Visa, MasterCard). The contract will require that the small business is, and will remain, compliant with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS compliance includes requirements for "security management, policies, procedures, network architecture, software design and other critical protective measures."[177]

If the small business is storing payment details in the cloud, to remain PCI DSS compliant, the small business must ensure that the cloud service provider is also PCI DSS compliant.[178] But again, in the absence of express statements from cloud service providers, an individual small business is unlikely to be able to adequately assess their cloud service providers for compliance.

Small businesses can partially avoid PCI DSS compliance issues by using services where the payments process and payments details are managed by the payments company (eg. PayPal), not the small business. In this case, small business has a different and less onerous contractual relationship with the payments company.

Health Services – Medical records are considered particularly sensitive. All health service providers must comply with the federal Privacy Act irrespective of business size. States and territories have similar record retention and security requirements for both the public and private sectors.[179]

Similarly, for businesses delivering health-related products and/or services into the United States, *Health Insurance Portability and Accountability Act*[180] (HIPAA) provisions dictate how health information must be stored to ensure the security and privacy of personal health information.[181]

7.6 Transborder Data Transmission

Information stored in the cloud may be stored anywhere across the globe, often redundantly across multiple locations.[182] If data are transferred across international borders, one or more international cross-border data transmission regulations may be activated with each country employing its own set of data protection and privacy laws.[183]

In Australia, the *Privacy Act* 1988 (Cth), National Privacy Principles, Principle 9 "outlines how organisations should protect personal information that they transfer outside Australia."[184] It restricts the transmission of personal information to a foreign country to circumstances *inter alia* where (for example):[185]

(a) the recipient is bound by contract or regulations with restrictions "substantially similar to the National Privacy Principles"; or

(b) the individual consents to their information being sent.

Similarly, the *EU Data Protection Directive* regulates the transfer of EU citizens' personal data beyond the European Union.[186] Under the *Directive*, implemented in each member state , companies are prohibited from transferring personal information to countries that do not have an equivalent level of regulatory protection.

7.7 Digital Forensics & e-Discovery

The whole issue of e-Discovery compliance could be problematic for small business, particularly those located in foreign jurisdictions.

Businesses must comply with legal discovery obligations—even if using cloud services to store their data—and put in place "a reasonable process for data to be retained, preserved, protected and disclosed."[187] Failure to do so may result in courts imposing strict penalties.[188, 189]

Many cloud service agreements stipulate the "choice-of-law" to be where the cloud service provider's headquarters' is located. In the case of Google, Amazon, Dropbox, 37signals, and many other cloud service providers that means the United States. Under the United States Federal Rules of Civil Procedure (FRCP), in order to "avoid unfavourable rulings" companies must:[190]

- know not only what data they are storing but also where it is stored;
- design, implement and adhere to policies to manage electronic data; and
- be able to prove compliance with such policies.

For small business the cost of even domestic legal proceedings is substantially beyond reach. In the event of even more cost-prohibitive overseas legal proceedings, together with such complex and burdensome FRCP compliance requirements, even the

relatively simple, preliminary e-discovery process is likely to be financially crippling for any small business.

7.8 Conclusion

The vast majority of small businesses are struggling simply to make next month's payroll. They turn to cloud computing to smooth cash flows and minimize personnel distractions, enabling them to dedicate more time and resources to the sharp-end, ie. developing new products and services, marketing and above all making sales.

But a complex, ever changing environment of interrelated and overlapping state- and national-level domestic and international regulations—often designed with a pre-cloud era in mind—threaten to undermine the appeal of cloud computing services for all but the biggest corporations.

Small business simply does not have the resources or skills to identify and understand the implications of the myriad regulations, and even less capability to measure cloud service provider compliance. The net result is blind ignorance, and frequent and unwitting non-compliance, eg. using Dropbox to store a business' financial records.

Even if small businesses were made aware of the facts, given their unique circumstances—their limited bargaining power and frequently tenuous financial position—they have little choice but to continue on and run the risk of being penalized for non-compliance.

8 Small Business & Cloud service providers – Contractual terms & conditions

8.1 Boilerplate Agreements – The only real option for small business

> *Cloud customers with so much at stake ought to possess sufficient bargaining power to have limitation on liability clauses removed from their contracts. Yet small start-up businesses with significant quantities of valuable information do not have this luxury and are often left with a boilerplate clickwrap agreement.*[191]

For larger business or government customers, limited liability and other clauses may be open to negotiation and customization, and (if ultimately necessary) be challenged in court. Small business—unlike larger organisations—will have wildly varying technical and legal resources to consider, and particularly limited bargaining power to negotiate (and almost no resources to challenge), such terms.[192] Small business must therefore typically accept boilerplate "click-wrap" agreements[193]—where the customer is held to have accepted the terms of the agreement by clicking "I Agree" on a web page—on a "take it or leave it basis" with no opportunity to negotiate terms.[194]

> *Faced with a standard form contract presented on a take it or leave it basis, the [small business] has little real choice but to acquiesce. To walk away is often a futile gesture as the [small business], on seeking to deal with another corporation, is in all likelihood going to be faced with a similarly drafted standard form contracted presented on a take it or leave it basis.*[195]

Nevertheless, even for big business, "customers of a cloud computing offering can expect less flexibility around [contractual terms and conditions] and operational matters."[196, 197]

8.2 Choice-of-Law – Usually the cloud service provider's HQ

Small business is not only unfavourably positioned relative to big business, but also vis-à-vis the consumer. Compared with the consumer, depending on the relevant legal jurisdiction, small business also has limited access to consumer protection laws. Accordingly—assuming clear and otherwise enforceable terms and conditions—the choice of law and applicable legal jurisdiction can have a significant impact on a small business and its capacity to render a contract enforceable.[198]

Cloud service providers are frequently large, multinational organisations (eg. Google, Amazon). The choice of legal jurisdiction may be (and often is) set to the cloud service provider's headquarters (eg. California or Washington).[199] Rarely it may be the jurisdiction of the customer, or something entirely different again.[200] For example:

> *If you are domiciled in: … a Country in Asia or the Pacific Region, other than Japan … you are contracting with: … Salesforce.com, Singapore Pte Ltd, a Singapore private limited company. The governing law is: … Singapore. The courts having exclusive jurisdiction are: … Singapore.*[201]

Litigation places a significant burden on any organisation, and is often beyond the reach of resource constrained small businesses. As geographic distances and

differences in legal jurisdiction increase, litigation costs quickly become prohibitively expensive.[202] Setting the legal forum to another country—as is commonly the case with cloud computing contracts—renders even the most basic form of legal proceedings essentially outside the financial and resource capacity of all but the most prosperous small businesses.

Enforceability of Choice-of-Law Clauses Unsettled – In terms of enforceability of the clause *per se,* that remains an open issue for Australian courts. In the United States, there is some evidence that in broadly similar agreements:

> *courts have been unwilling to enforce onerous arbitration and choice of forum clauses against consumers, even when the consumer agreed to the standard form imposing such requirements.*[203]

Typically such clauses have been struck down in the United States on the basis of either procedural or substantive unconscionability.[204] However, there are also many counter examples, such as *Feldman v Google*[205] and *In re RealNetworks, Inc. Privacy Litigation*[206] respectively enforcing forum-selection and arbitration clauses. In 2002, in reviewing nine United States click-wrap and "browse-wrap" cases addressing the enforceability of forum-selection clauses, Kaustuv Das found seven enforced the clauses.[207] In Australia however the issue remains open and unresolved.

Summary – In the absence of cloud service provider agreements with "local" (ie. Australian) jurisdiction—rendering enforcement issues moot—for small business, such judicial uncertainty represents the potential for prohibitive legal expense and therefore commercial uncertainty. It, along with limitations of liability clauses (see below), threaten to transform cloud computing into a form of commercial Russian roulette. Were knowledge of such terms and their potential practical commercial implications to become more widespread amongst the small business community, they would serve only to render cloud computing significantly less attractive.

8.3 Liability & Limitations of Liability – Service providers seek to absolve themselves of substantially all liability

> *[A cloud service provider] could purposefully delete its customers' data or shut down its … websites, leaving the aggrieved customers with no cause of action and no right to recover.*[208]

Businesses of all kinds should look closely at any terms in cloud service provider agreements purporting to limit or exclude liability. But rarely are the terms of a cloud agreement closely scrutinized. In 2010, as April Fool's Day joke, the British online gaming store GameStation inserted the following clause into its online agreement:

> *By placing an order via this Web site … you agree to grant [GameStation] a non transferable option to claim, for now and for ever more, your immortal soul.*[209]

GameStation also provided a separate button enabling astute readers to "click here to nullify your soul transfer" and be rewarded with a £5 coupon. Only 12% of subscribers on April Fool's Day nullified their "soul transfer" to receive the coupon![210]

Terms and conditions of cloud computing click-wrap agreements resemble traditional "shrink-wrap" software agreements, significantly limiting service provider liability,[211] but with the added risk associated with the high value and volume of business-critical data stored in the cloud.[212] But for small business—without the ability to negotiate

such clauses—what do these boilerplate clauses really mean? Do they genuinely substantially exclude service provider liability?

Cloud Service Providers Substantially Exclude Liability – Commonly, cloud service providers seek to absolve themselves of all, or substantially all, direct,[213] indirect, consequential or economic liability beyond monthly subscription fees.

For example, from Google Apps, Terms of Service:

> *Google … shall not be liable to you for any direct, indirect, incidental, special consequential or exemplary damages which may be incurred by you, however caused and under any theory of liability.*[214]

Similarly, Amazon Web Services, Customer Agreement:

> *[Amazon Web Services] will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of Your Content.*

Click-wrap Limitations of Liability Likely Enforceable – In the United States, until *ProCD v Zeidenberg*[215] (1996) in the pre-Internet era, courts rendered similar shrink-wrap agreements unenforceable,[216] often as an unconscionable "contract of adhesion."[217, 218] Clearly there are distinctions that can be made between shrink-wrap and click-wrap agreements, eg. access to terms prior to acceptance can be quite different. However, if more recent decisions in the United States are any indication, click-wrap agreements—and their limitations of liability clauses—are prima facie enforceable, independent of whether or not the customer has read the terms.[219]

> *[Courts in the United States] have unanimously found clicking is a valid way to manifest assent since the first clickwrap agreement was litigated in 1998. … [A]bsent fraud or deception, the user's failure to read, carefully consider, or otherwise recognize the binding effect of clicking 'I Agree' will not preclude the court from finding assent to the terms.*[220]

8.4 Consumer Protection Laws & Potential Legislative Solutions – Consumer protection laws to the rescue for small business? Potentially.

Despite cloud service providers' attempts to avoid substantially all liability, depending on the relevant governing law of the cloud contract (see below, Governing Law & Legal Jurisdiction), various species of common law and state or national legislation may imply new terms, weaken or even strike down existing terms in the contract.

Consumer Protection Laws – Jurisdictionally-specific consumer protection legislation and/or common law may serve to protect small business operators seeking to benefit from the cloud:

- *In Australia* – If the agreement is governed by Australian law (see Choice-of-Law below)—under the proviso that (a) the services do not exceed $40,000 or (b) are "of a kind ordinarily acquired for personal, domestic or household use or consumption"[221]—Schedule 2, *Competition and Consumer Act* 2010 (Cth) (the CCA) will imply various guarantees.

  For example: The CCA guarantees that the service will be "rendered with due care and skill."[222] Further, if the consumer makes a particular purpose known to the vendor, the CCA guarantees that the service "will be reasonably fit for that purpose."[223] If, however, the proviso does not apply, cloud service

providers may limit their liability to resupplying, or paying the costs of resupplying, the service[224] – consistent with the Service Level Agreements and limited liability clauses of many cloud service provider agreements.

Fortunately, for small businesses, most cloud services will in practice come under the A$40,000 proviso. Dropbox's cloud storage service has a 100GB "Pro Account" for US$9.99 per month.[225] 37signals' most expensive Basecamp project management service (managing unlimited projects) is US$150 per month.[226] Salesforce's "Unlimited" account sells for US$250 per month.[227]

- *In England – Kingsway Hall Hotel v Red Sky IT (Houslow)*[228] may provide early indication that small (and medium) sized businesses are not without consumer-like protection. Seeking to rely on its standard limited liability terms, Red Sky IT—a specialist non-cloud, software provider—was held to have provided software the "was not of satisfactory quality or fit for its purpose"[229] to Kingsway Hall Hotel—a non-specialist business customer.

  Further, *GB Gas Holdings v Accenture*[230] may provide a basis (in England at least) for dismissing or at least curtailing service provider attempts to insulate themselves from "losses consequential on service failure."[231]

Possible Legal Doctrines – Several important legal doctrines—if adapted to the unique circumstances of cloud computing—may also serve to aid potentially dissatisfied small businesses using cloud services:

- *Unconscionability*[232] – Some argue for a "rejuvenation of the doctrine of unconscionability" to come to the aid of cloud computing customers:[233]

  > *Just as courts [in the United States] used unconscionability to strike down onerous clauses during the early days of the Internet, the same should be done during the infancy of cloud computing. In rejuvenating this doctrine, the courts might prevent harm to the cloud computing market while providing adequate safeguards to its customers.*[234]

  However, such a perspective relies heavily on judicial activism in cases of substantive (rather than procedural) unconscionability.[235]

  Australian courts have recognised the *existence* of both procedural unconscionability (unconscionable conduct leading up to the formation of the contract) and substantive unconscionability (unfairness of contractual terms and/or their enforcement).[236] But, unlike their American counterparts,[237] it is unclear whether Australian courts are willing to intervene in circumstances of substantive unconscionability.[238] While s.22, *Australian Consumer Law* sets out guidelines for assessing unconscionability, including both procedural and substantive matters, it is remains unclear as to courts' interpretation.

  Irrespective of which, it is unclear whether statutory reinforcement of unconscionability is an adequate solution. As Frank Zumbo[239] puts it:

  > *Statutory prohibitions against unconscionable conduct are of little use, as they are difficult to enforce and deal only with individual examples of offending conduct. Significantly, a finding of unconscionable conduct in one relationship may not necessarily promote better conduct in another relationship.*[240]

- *Exclusion Clauses* – Such limitations of liability clauses may be open to attack as exclusionary clauses. If this is the case, it may be difficult to identify the service providers as providing adequate notice for the purposes of an exclusion clause,[241] perhaps requiring something comparable to Lord Denning's "red hand test."[242] But again, the issue remains one of bargaining power. Awareness of a term and its potential consequences is tantamount to useless without the bargaining power to negotiate/renegotiate terms; a power small business simply does not have.[243]

A New Legislative Approach – Others advocate a wholly new legislative approach to electronic contracts.[244] Clapperton and Corones cite the Australian Communications Industry Forum Industry Code for Consumer Contracts (ACIF C620:2005) (ACIF Code)[245] as precedent.[246]

The ACIF Code in turn draws upon Part 2B, *Fair Trading Act* 1999 (Vic) which seeks to squarely address unfair terms in consumer contracts.[247] The objectives of the ACIF Code are:[248]

> *(a) to identify and prohibit the use of unfair terms in Contracts;*
>
> …
>
> *(c) to state the minimum requirements for the format and structure of Contracts and to encourage the use of plain language.*

For the purposes of a small business, under the ACIF Code, "a term in a Contract must not be unfair"[249] if the small business:[250]

(a) acquired telecommunications products and services from a supplier;

(b) has not had a "genuine and reasonable opportunity to negotiate the terms of the Contract" with the supplier; and

(c) has or will have "an annual spend with the Supplier … no greater than $20,000."

When assessing whether a term in unfair, it is "relevant to consider whether the term has the object or effect of: (a) excluding or limiting liability of the Supplier …"[251]

Although non-binding *per se*, the ACIF Code is not without teeth. It is registered under s.117, *Telecommunications Act* 1997 (Cth), permitting the Australian Communications and Media Authority to compel compliance in the first instance or ultimately issue a pecuniary penalty.[252]

In the End, Uncertainty Reigns – What is clear from the above, is that there exists significant uncertainty about the potential enforceability of cloud service provider contracts and limitation of liability clauses. Contractual uncertainty requires advice and interpretation, ie. lawyers. Lawyers are expensive—particularly in relation to such an untested area of the law—and beyond the means of all but the most financially well endowed small businesses. The net result is likely to be that small businesses will:

(i) accept the boilerplate agreement 'as is' hoping that nothing untoward happens, and seek out solutions to bandaid over perceived risks (eg. maintaining their own local data backups or relying on the possibility of business interruption insurance); or

(ii) avoid the cloud altogether—and all of its significant potential operational and commercial benefits.

Summary:

- If the governing law is Australian and if cloud services do not exceed A$40,000, small businesses may receive some protection under the Australian Consumer Law embodied in Schedule 2, *Competition and Consumer Act* by implying certain guarantees into the service agreement.
- English common law may provide some indication as to the limited enforceability of cloud service provider limitations of liability.
- Equitable principles, such as unconscionability, could possibly be applicable—particularly in relation to a technically unsophisticated small business—but are likely to require an expansion of judicial activism into the field of substantive (and not just procedural) unconscionability.
- Further, legal enforcement on the basis of unconscionability and exclusionary clauses operates on a case-by-case basis. It may therefore be insufficient to compel cloud service providers with superior bargaining power to improve conduct across all relationships.
- A *sui generis* approach may be more optimal – perhaps combined with restructuring around legislatively enforced unconscionability.
- The ACIF Code may provide a basis for legislative intervention.
- At present uncertainty dominates the enforceability of exclusion clauses, with the likely net effect of applying a brake to the adoption of cloud computing services by small business.

8.5 Cloud Service Provider Representations – Cannot be misleading or deceptive

Many unsophisticated and time-poor small business owners looking for a quick, cost effective solution may be encouraged by representations of security, data recovery and other services made on cloud service provider websites or through subsequent discussions. However, cloud service providers will often seek to exclude such representations from the terms of the contract,[253] for example:

> *No advice or information, whether written or oral, obtained by you from ZoHo, its employees or representatives shall create any warranty not expressly stated in the [Terms of Service Agreement].*[254]

Accordingly, cloud service providers seek to declare such "advice or information" as "mere representations," and not legally binding. Under Australian law, however, such public or private representations cannot be excluded from the terms of the agreement if they constitute misleading or deceptive conduct.[255] Nevertheless, the potential of such advice or information to constitute "mere representations" simply serves to add to the legal uncertainty pertaining to cloud agreements.

8.6 Service Level Agreements & Service Credits – A "sole & exclusive remedy," and a big issue for small business

> *If business-critical applications and data are accessed and stored via cloud services, the failure of the service, even for relatively modest amounts of time, can have significant impact.*[256]

Small Service Failures can have a Big Impact – The potential impact of the failure of cloud services is particularly relevant for small business operators with their inconsistent, often unpredictable cash flows. Larger organisations have more significant and homogenous cash flows and can typically ride-out a temporary service failure. For a small business however, the failure of services at the wrong time in their cash flows can have a devastating impact, with the ultimate potential to render the small business insolvent.

> *Being without access to key business data for a day or two – or even a few hours – could be devastating to small business.*[257]

Accordingly, Service Level Agreements (SLAs) should be of particular importance to small business operators.

SLAs a "Sole & Exclusive Remedy" for Service Failure – While most cloud service providers seek to absolve themselves of substantially all direct and indirect liability, some cloud service providers provide limited prescribed compensation—typically as the "sole and exclusive remedy"—through SLAs for service failures.

SLAs can take many forms, but invariably do not incorporate any compensation for lost revenues, etc. incurred by the small business. Typically, the small business's recourse is "solely and exclusively" limited to being assigned "service credits."[258] The quantum of assigned service credits is a function of the nature and extent of service downtime. For example:

> *[Google Apps] will be operational and available to Customer at least 99.9% of the time in any calendar month (the "Google Apps SLA"). If Google does not meet the Google Apps SLA … Customer will be eligible to receive Service Credits … This Google Apps SLA states Customer's sole and exclusive remedy for any failure by Google to meet the Google Apps SLA.*[259]

Onus on Small Business to Monitor & Apply for Service Credits – Most SLAs exclude planned downtime (eg. to undertake scheduled maintenance, etc.), internet failure, or where the downtime is less than a minimum period (eg. 10 minutes).[260] But often the onus rests with the customer—the already time- and resource-starved small business—to monitor cloud services for any downtime and apply for service credits within a specified period:

> *In order to receive any of the Service Credits described above, Customer must notify Google within thirty days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Customer's right to receive a Service Credit.*[261]

Rarely, the cloud service provider themselves may monitor and apply credits:

> *[provider] will monitor the availability of each Virtual Private Data Centre, and will automatically issue any credit that is due. In addition, you may report any instance of unavailability.*[262]

Summary:

- cloud service downtime can have a potentially devastating impact on a small business;
- Service Level Agreements (SLAs) that regulate the cloud service providers liability for service downtime:

(i) provide no real compensation—limiting liability to additional days of service—and

(ii) often place the onus on already time-starved small business to monitor the service and apply for what little compensation is available.

8.7 Variation of Terms – 'In cloud service provider we trust'; small businesses need to choose a cloud service provider with a reputation to protect

Part of the attraction of cloud services is their ability to be continuously updated and improved, responding to changes in technology and/or the regulatory environment. To effect these changes, cloud service provider agreements often grant the cloud service provider the discretion to unilaterally vary terms of the agreement from time-to-time obviating the need for ongoing agreements of amendment.[263]

As highlighted by Vincent, Hart & Morton, this implies an element of trust in the cloud service provider by the client, and "underlines the importance of selecting a vendor with an established reputation which it is unlikely to put at risk by a capricious use of the discretion."[264] This should be particularly relevant for small businesses considering cloud offerings and forced to accept boilerplate agreements.

8.8 Data: Location, Disclosure & Transfer – Location and (hence) jurisdiction is important for small business

> *As a customer, you don't know where the resources are, and for the most part, you don't care.*[265]

This may be the view of cloud service providers, but for their customers—particularly small business concerned about any additional expenses arising from additional compliance requirements, etc.—"where the resources are" can be a big issue. Exactly which courts and/or law enforcement agencies have jurisdiction to require data disclosures[266] may be subject to the physical location of client data stored in the cloud. For a resource-constrained small business, just as choice-of-law is important, so too may data location be equally important. As the Electronic Frontiers Foundation put it highlighting the cost implications of geographically-remote legal action:

> *A small San Francisco ISP served with [a warrant served under the PATRIOT Act issued by a New York court] is unlikely to have the resources to appear before the New York court that issued [the warrant].*[267]

Data Location – Despite the importance of data location, few cloud service providers make mention of it[268] – possibly because (i) they themselves may not know, and/or (ii) it varies from time-to-time.

Amazon's S3 (Simple Storage Service) is a rare exception, enabling subscribers during the sign-up phase to nominate one of four regions to store their data and/or applications:

> *You may specify the AWS regions in which Your Content will be stored … We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities.*[269]

But even Amazon does not expressly define or incorporate its "AWS regions" in its terms and conditions. And while many United States-based cloud service providers will often assert compliance with US-EU Safe Harbor Privacy Principles—indicating adherence with the more rigorous European Union standards of privacy protection, etc.—the majority of cloud service provider agreements are silent on the issue of data location and data transfer.

Data Disclosure – In common with other organisations, small business may also be concerned with the circumstances in which a cloud service provider may disclose their data to third parties:

- *Court Ordered Disclosures & Law Enforcement Agencies* – Substantially all cloud service providers include clauses stating that they will disclose customer data collected and stored on their system to third parties in response to a court order. *Where legally permitted*,[270] some cloud service providers (eg. Salesforce) will provide prior notice of the court order to the relevant customer and may provide "reasonable assistance" to contest the disclosure order.[271] Others have a slightly lower threshold, permitting disclosures upon good faith requests by law enforcement agencies.
- *Lower Thresholds of Disclosure* – Other cloud service providers may permit the disclosure of customer information under a broader set of circumstances, including protecting the interests of the cloud service provider:

  > *[Dropbox] may disclose … files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is necessary to … (d) to protect Dropbox's property rights.*[272]

Data Transfer – Issues may arise surrounding which jurisdictions data may be transferred to/from, and the security of data in transit:

- *Limitations of Data Transfer* – Commercial and private data may be stored in one or more locations, and may vary over time. Cloud customers may have very little control over exactly where their data is stored and/or transferred to.

  > *… As part of providing the Services Google may transfer store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services Customer consents to this transfer, processing and storage of Customer Data.*[273]

  Depending on the nature of the data transferred, what the target jurisdiction is and the nature of the privacy and other regulations in the target jurisdiction, the cloud customer may have manifold regulatory compliance issues. For small business, this could mean potentially prohibitive personnel time in administrative and regulatory reporting.
- *Data Transfer Security* – In the absence of a private, secure network, any data transfers will occur over the publicly accessible internet. But what is the security of the data in transit? Bradshaw *et al* quote 37signals' Terms & Conditions which openly state that:[274]

  > *You understand that the technical processing and transmission of the Service, including your Content, may be transferred unencrypted and involve (a) transmission over various networks;*

> *and (b) changes to conform and adapt to technical requirements of connecting networks or devices.*

In comparison, Bradshaw *et al* also quote Dropbox's website (not its Terms & Conditions):[275]

> *Dropbox takes the security of your data very seriously. Everything you store on Dropbox is encrypted both in transmission and storage. Nobody can access your files unless you choose to share them yourself.*

For the IP-oriented small business struggling for survival, the potential risk of losing business-critical information in transit may be too great.

8.9 Data: Data Integrity, Privacy & Security – Typically the burden of the client, undermining a key benefit of cloud computing for small business

> *A flaw in the Google Docs application, now fixed, had the effect that some users inadvertently shared some of their documents.*[276]

Cloud computing relies on sharing consolidated, centralised resources of hardware and/or software services to a wide range of client users. Therefore, there is a risk, either via malicious intent or system error, that other (potentially competing) organisations may gain access to client data.

Small businesses are particularly attracted to highly cost effective and scalable cloud-based services like SalesForce.com.[277] But as individual cloud-based services grow in scale and popularity,[278] they become an increasingly attractive target for cybercriminals seeking to steal highly valuable client and customer information. It is little wonder that security remains the pre-eminent concern for all cloud users.

> *In early 2010, Microsoft undertook a survey to assess business leaders' attitudes to cloud computing. … more than 90 per cent [of respondents] were concerned about security … and/or of privacy in the cloud.*[279]

Data integrity, privacy and security issues may be enforced via regulatory or contractual requirements. Among other things, it has been suggested that the privacy clause of the contract between the cloud service provider and the client should stipulate:[280]

- service provider mechanisms for safeguarding client data; and
- procedures for alerting the client in the event of a privacy breach.

Most Cloud Service Providers are Vague on Security – Some cloud service providers will openly declare that they use data encryption, but not necessarily incorporate such representations as terms in the cloud service provider agreement. For example, Dropbox states in its "Security Overview" that:

> *[Dropbox] encrypt[s] the files that you store on Dropbox using the AES-256 standard, which is the same encryption standard used by banks to secure customer data.*[281]

But it fails to reference or otherwise incorporate such representations into its Terms of Service[282] or Privacy Policy.[283]

Similarly, in its "Security Statement," Salesforce declares:

> *When you access [Salesforce.com's] site using industry standard Secure Socket Layer (SSL) technology, your information is protected using both server authentication and data encryption, ensuring that your data is safe, secure, and available only to registered Users in your organization. Your data will be completely inaccessible to your competitors.*[284]

It too fails to include any such clause in its Master Subscription Agreement.[285]

Nevertheless, as discussed in the regulatory aspects of data security, many cloud service providers fail to provide openness or sufficient detail in their contractual obligations. Many cloud service provider agreements appear deliberately vague about the topic of data security:

> *[Google] adhere[s] to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data …*[286]

In 2009, the Electronic Privacy Information Centre (EPIC) filed a complaint with the US Federal Trade Commission (FTC) alleging Google did not adequately safeguard the confidential information of its users.[287] Together with Google's data security clause, it provides little comfort for current or potential customers.

Most Service Providers Shift the Security Burden onto Clients – The bulk of cloud service providers go further, actually disclaiming liability for data integrity and confidentiality.[288] Worse still, some cloud service providers may seek to shift the ultimate burden of security on to the customer, the small business:

> *[the customer is] solely responsible for procedures and controls regarding encryption and backup of all content and for the implementation of these procedures and controls. … they [the customer] bear sole responsibility for adequate security, protection and backup of [customer data and applications].*[289]

It is only prudent that a small business maintains some level of independent data redundancy in the event of a security breach or failure of service. However, to burden the small business with "sole responsibility for … encryption and backup" would seem not only excessive but to substantially defeat a key, promoted benefit of cloud computing.[290] And, if more widely known, such terms and conditions would serve to substantially undermine cloud service adoption.

8.10 Data: Multiple Party Delivery of Services – Cloud service providers are likely to share client data to third-parties

Data from cloud computing customers may flow beyond the principal contracting cloud service provider on to other third parties. For example - advertising supported cloud computing services operate by permitting the cloud service provider to direct targeted advertising to its customers. By necessity, it means forwarding at least some customer data to third parties to deliver the targeted advertising.

Several issues may also arise with the use of cloud subcontractors. For example: Dropbox—operating a "freemium" business model—provides users with encrypted, cloud-based file storage and synchronization solution, but actually uses Amazon's Simple Storage Solution (S3) to store user data.[291]

More generally, exactly which cloud subcontractors are used in what jurisdictions may vary from time-to-time depending on availability and price. And, in the event the cloud service provider goes bankrupt, it is unclear what rights subcontractors have in respect of the small business' data.[292]

While small businesses should endeavour to check what data are provided to third parties under what circumstances,[293] getting a satisfactory answer—in terms of compliance obligations, etc.—may be particularly difficult.

8.11 Data: Intellectual Property – Service providers rarely claim any title in client content

The importance of intellectual property (IP) varies tremendously from business-to-business. For a large pharmaceutical company, IP and its protection is core to the business. For a simple import/export business, it is not.

Small business runs the gamut of products and services: from the provision of physical services (eg. plumbers, personal trainers), import and distribution businesses, and physical shop fronts; through to the delivery of more intangible services, such as consulting services (eg. providing business, technical, medical or legal advice), graphic and industrial design services, and software development.

For those operating more intangible business services—particularly small businesses involved in the design of new products and/or services (typically for other, larger organisations)—protecting one's IP is key.

Fortunately, it is extremely rare —verging on non-existent—for a cloud service provider to assert any IP rights over client data. Dropbox's Terms of Service provides an example:

> *… you provide us with information, files, and folders that you submit to Dropbox (together, "your stuff"). You retain full ownership to your stuff. We don't claim any ownership to any of it.*[294]

In an ongoing matter before the Criminal Court of New York City, Twitter has gone so far as to issue a motion to the Court arguing that its Terms of Service "make absolutely clear that its users own their content" and that the "Terms of service expressly state: 'You retain your rights to any content you submit, post or display on or through the service'."[295]

What is more common, however, is the cloud service provider's reservation of the right to republish or distribute customer data to third parties for the purposes of providing the service (see above, Multiple Party Delivery of Services).[296]

8.12 Data: Data Portability, Service Provider Lock-In & Termination – Yet another big issue for small business

> *A survey of cloud computing customers by RightScale found their main concern was the possibility of being locked in to a cloud computing provider.*[297]

Larger organisations are more likely to have the technically skilled personnel capable of managing the transition of organisational data (and that of its customers) from one cloud service provider to another. For small businesses however—with few personnel, extreme time constraints, and often limited technical skills—switching cloud service providers is a potential nightmare, representing a significant barrier to cloud computing adoption.

Access to Data – Prima facie, there is no general legal requirement for cloud service providers to provide data export facilities before or after termination; it all depends on the nature of the agreement.[298] Contractual terms and conditions vary significantly regarding a cloud service provider's obligations upon termination. Some provide access to client data for a specified or "reasonable period" of time, others do not. Some entitle the cloud service provider to delete client data, while others leave open the issue of data retrieval – leaving the client to extract their data prior to termination.[299]

> *[Upon termination] … (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates for the applicable Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data …*[300]

It is imperative that small business owners understand what will happen to their data stored in the cloud prior to terminating the agreement. For example, some agreements permit the cloud service provider to delete all customer data immediately upon termination:

> *All of your Content will be immediately deleted from the [Basecamp Service] upon cancellation. This information can not be recovered once your account is cancelled.*[301]

Data Portability – For a small business, it is particularly important that the transition from one system or cloud service provider to another is as smooth and as simple as possible. Data portability is central to this. It is therefore important that an open or vendor-neutral data format is stipulated in the service agreement. Salesforce.com's Master Subscription Agreement provides an example:

> *Upon request by You made within 30 days after the effective date of termination … We will make available to You for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format. After such 30-day period, We shall … unless legally prohibited, delete all of Your Data in Our systems …*[302]

Yet such a vendor-neutral or open-standards approach is rarely expressed amongst cloud service provider agreements. Even more rarely will service providers provide any form of technical assistance with transitioning out; technical assistance that small business so often desperately lacks.

Termination & Termination for Cause – Cloud service providers may reserve the right to unilateral termination.[303] Commonly client access to data is eliminated if termination is "for cause" or subscription fees are not up-to-date.[304] For small business, this could essentially constitute holding the small business to ransom.

Vendor Bankruptcy – Very few cloud service provider agreements make mention of client rights (particularly in relation to third parties) in the event of service provider bankruptcy. Legally, very few cloud service providers claim proprietary rights in client generated data (see above, Data: Intellectual Property). But in practical terms, just what this means for small businesses—without resources to chase liquidators, third parties, etc.—is unclear.

Third Party Technical Consultants – Another more costly alternative for small business' lacking more technically skilled personnel, is to import the skills,

contracting third party IT consultants to undertake the evaluation and/or management of the transition from one cloud service provider to another.

Minimizing the Need to Switch – Better, more attractive services are a common motivation for switching cloud service providers. If, however, cloud services are continually improved and priced to be competitive, such motivations may become less of an issue. Accordingly, small businesses in particular should look to clauses to ensure they receive the latest functional updates.[305]

Summary:

- Service provider lock-in is a big issue for all organisations, but particularly for small business;
- Unless termination is "for cause" or subscription fees are not up-to-date, clients are typically able to extract their data from the service provider for a "reasonable period" after termination;
- It is important that the extracted data is in an open- or vendor-neutral standard to smooth the transition from one cloud service provider to another;
- The need to switch may be reduced if the cloud service provider is obligated to deliver competitive service updates.

8.13 Data: Data Deletion Post-Termination – No standard approach by cloud service providers

> *… customers will be concerned as to whether data they entrust to the Cloud service provider will ever be deleted comprehensively from the Cloud. … Were this perception to become widespread, it could become a significant barrier to the large-scale take-up of [cloud services].*[306]

The flip-side of termination is the issue of data deletion: Does the cloud service provider provide an assurance that—upon termination or a specified period thereafter—the small business' data will, in fact, be irrecoverably deleted from the cloud?

Some cloud service provider agreements leave the issue open, simply stipulating (for example) that: "during the 30 days following termination: (i) we will not erase any of Your Content as a result of the termination …"[307] The clause states what the cloud service provider will not do; it does not apply any positive obligation on the cloud service provider to delete customer data.

Conversely, the Google Apps for Business (Online) Agreement or the Salesforce Master Agreement (described above) obligate the service provider to delete all customer data after a specified period of time.[308]

But specific assurances that data will be deleted irrecoverably are rare. Simon Bradshaw *et al*[309] quote 3Tera as an example:

> *All customer data remaining after the cancellation date will be destroyed for security and privacy reasons.*[310]

Summary – Despite being a potentially important issue for small businesses (particularly those more IP-oriented organisations), data deletion is currently managed in a highly inconsistent but generally poor manner by cloud service provider agreements.

Unlike many other terms, providing a cloud service provider obligation ensuring data deletion would not appear to be overly burdensome upon the service provider yet deliver significant client satisfaction, eliminating a "significant barrier to large-scale take-up of [cloud services]."[311]

8.14 Data: Data Recovery & Business Continuity

> *Many small businesses lack the resources and/or IT expertise to regularly back up their day-to-day business data off-site. Yet when disaster strikes, … millions of the country's small businesses are the most vulnerable to data loss and corresponding loss of revenue.*[312]

Large organisations have resources to maximise business continuity through redundancy – they often have multiple offices and typically maintain backups of critical data and IT infrastructure. Small business rarely has this luxury. But cloud computing holds out the promise "to rapidly recover from any outage and to greatly reduce the down-time."[313]

Therefore, data recovery and business continuity aspects of cloud service agreements of particular interest to small businesses. But as technology journalist, Robert (Bob) X. Cringley, warns novice cloud computing users:

> *It might surprise many users [of cloud services] to know there are firms that sell cloud storage and do not back it up. … If something happens to [the cloud service provider's] data center, they could probably not recover your data. … you had better make sure your service provider won't let you down.*[314]

Ideally the service provider agreement would provide assurances that adequate testing is done on a regular basis and define the extent to which the client can participate and/or monitor such testing.[315] However, it seems highly unlikely that a large-scale cloud service provider would be willing to permit thousands, possibly tens-of-thousands, of clients to receive such rights.

Service provider agreements tend to be largely devoid of any express terms relating to regular and adequate testing.[316] Salesforce and Google Apps (standard and premier services) provide possible exceptions:

> *[Salesforce] shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data.*[317]

and:

> *Google has implemented at least industry standard … procedures to … protect against anticipated threats or hazards to the security or integrity of Customer Data.* [318]

Despite being an important benefit of cloud computing—particularly to small business—the lack of clear, express terms providing assurances regarding data recovery and business continuity serves again only to undermine a key attraction of cloud computing for small business.

8.15 Data: Data Loss – What happens if the cloud service provider can't recover your data?

> *Regrettably, based on [Microsoft's] latest recovery assessment of their systems, we must now inform you that personal information stored [in our cloud] almost certainly has been lost as a result of a server failure at [Microsoft].*[319]

The Microsoft example is (unfortunately) not wholly unusual.[320] And while cloud service providers often have detailed data recovery and business continuity plans, things still go wrong. A December 2011 survey of 300 companies across the United States conducted by Computer Associates found that:

> *100% of organizations surveyed have experienced application and data loss over the last year. The most common cause of data loss is IT systems failure, eg. hardware or network failure (78%).*[321]

But rather than being seen as decreasing data security, cloud computing is often viewed as a means of increasing it, especially amongst those less technically sophisticated small businesses.[322]

Unfortunately, it is rare to find terms and conditions in relation to cloud service provider data loss. Instead, given the expansive language of limited liability clauses, cloud service providers purport to be substantially devoid of any legal obligation regarding loss of a customer's own data. As Timothy Calloway put it:

> *[A cloud service provider] could purposefully delete its customers' data … leaving the aggrieved customers with no cause of action and no right to recover.*[323]

8.16 Free Accounts – You get what you pay for

Many cloud service providers employ a "freemium" business model to attract entry-level customers, where the basic service is provided free of charge with additional functionality attracting subscriptions fees.[324] Looking for every opportunity to survive, cash-strapped small businesses (unlike larger organisations) are likely to be particularly attracted to "free." But nothing is ever genuinely free.

Termination without Notice – Many cloud service providers provide quite different terms and conditions for "free" versus "for-fee"/premium accounts.[325] For example: Some cloud service providers retain the right to "terminate Free Accounts at any time, with or without notice."[326]

Automatic Termination of Inactive (Free) Accounts – A small business may only use a service intermittently. Some cloud service providers—such as Dropbox which provides 2GB online data storage free—reserve the right to automatically terminate service if an account has remained inactive for a specified period of time.[327]

Practical Implications – Such terms and conditions are common amongst free cloud service offerings. But even clear, advanced knowledge of such clauses may do little to aid the small business: they have limited vendor options, and almost non-existent negotiating power to amend term(s). Similarly, providing "reasonable warning" of termination (in the absence of direct assistance and/or open standards) may do little better: small businesses rarely have access to the necessary technical skills to transition out of a particular cloud service provider's service.

Accordingly, without careful consideration prior to entry, small businesses run the very real risk of having their businesses and their livelihoods devastated by the service provider's power to unilaterally terminate the client's account.

9 Small Business, Their Customers & Business Insurance – The potential for insurance to cover civil liabilities

> *It's becoming clear that [IT professionals] are really looking for [two] distinct things when they evaluate cloud technology. The first is the solution itself … The second is something like an insurance policy to protect them if anything goes wrong … what you might call "Cloud Insurance."*[328]

Existing Recourse is Inadequate – As businesses increasingly turn to the cloud, business will increasingly be subject to interruptions "in the cloud."

As cloud service provider agreements stand, in the event of service interruption or failure and/or data loss, the small business has (in theory) two lines of recourse, both highly unsatisfactory: (i) Service Level Agreements with deficient service credits (see above, Service Level Agreements & Service Credits), and (ii) prohibitively expensive legal action.

The question therefore is: Can businesses rely on existing insurance policies to cover such outages or must they seek out new forms of insurance?[329]

Existing Business Insurance Unlikely to be Sufficient – Australian small businesses typically purchase standard-form "office pack" or "business pack" insurance policies, frequently including business interruption (BI) insurance. BI insurance is generally limited to physical damage to the insured's own facilities on premises,[330] substantially excluding the applicability of BI insurance to cloud-based interruptions. Furthermore, insurance policies often expressly exclude internet-related compensation:

> *We [the insurance company] do not cover losses caused by or resulting from the partial or total failure, malfunction or loss of use of any electronic equipment, computer system … or other similar device due to: … (c) the inability to receive, transmit or use data; or (d) the impact of … the functioning or malfunctioning of the internet … or of any internet address, website or similar facility …*[331]

Therefore, small business is unlikely to obtain any satisfaction from existing standard-form office or business pack insurance policies.[332]

Existing Cyber Liability Insurance Unlikely to be Applicable – Australian insurance companies are now also offering "cyber liability policies" to compensate in the event of (for example) "e-Theft Loss" or "e-Communication Loss" or even "e-Business Interruption." However, such policies are again restricted to losses derived from the insured's own facilities, not third-party suppliers, eg. cloud service providers. The policies pay-out in the event of (eg) business interruption caused by the insured's website going down where the website is run on the insured's own, on-premises servers.

Accordingly, they appear to provide compensation in the event that a virus, possibly DDoS, or other similar cyber crime occurs on the insured's own in-house equipment. It is unlikely that such cyber liability insurance would cover similar attacks where the small business's website is hosted externally.

Therefore, again, in the context of compensating for losses caused by failures in the cloud, existing cyber liability insurance is unlikely to meet the cloud-related needs of small business.

ISR & CBI Insurance – Another species of insurance (primarily available to larger organisations) is Industrial Special Risks (ISR) insurance. ISR insurance comes in many flavours, including contingent business interruption (CBI), the result of damage to suppliers' property.[333] For example:

> *Loss resulting from interruption of or interference with [the insured's business] in consequence of Damage to property at the specified premises anywhere in the world of any producer [ie. any supplier of goods or services used by the insured] … identified in the Schedule … shall be deemed to be loss resulting from Damage to property used by the Insured…*[334, 335]

Such "damage to the specified premises anywhere in the world" could include server farms and other infrastructure.[336] However, such insurance is prima facie limited to physical damage to suppliers' infrastructure.[337] It therefore provides cover in the event of (eg) a lightning strike rendering a cloud service provider's server farm temporarily inoperable.[338] But it would not cover damage resulting from, for example, a software bug[339] or computer virus.

What is "physical loss or damage"? – What constitutes "direct physical loss" under business interruption insurance continues to be debated.[340] CBI insurance appears to rely on physical loss or physical damage. Traditionally, insurance companies and courts have been reluctant to equate software failures and data loss with physical loss, generally concluding that "damage to software or data [alone] does not constitute 'direct physical loss'" for insurance purposes.[341] Discussions with insurance brokers would tend to indicate that this is strongly the case in Australia.

However, in the United States at least, there appears to be growing judicial support for a more expansive view that software failures and data loss can equate to physical loss for the purposes of an insurance policy. For example, *American Guarantee & Liability Ins. Co. v Ingram Micro, Inc.*[342] held that:

> *The Court finds that "physical damage" is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.*[343]

Similarly, in *Southeast Mental Health Center, Inc. v Pacific Ins. Co Ltd.*, the court held that "corruption of the [insured's] computer constitutes 'direct physical loss of or damage to property' under the business interruption policy."[344] Importantly, *Wakefern Food Corporation v Liberty Mutual Fire Ins. Co.*[345] held that "*from the perspective* of the millions of customers … the system certainly suffered physical damage …"[346] (emphasis added)

The principal concept from these decisions is that whether there was physical damage should be assessed in terms of whether there was functional impairment from the perspective of the insured.[347]

"Cloud Insurance" is a Viable Alternative – Depending on the actual or implied terms of the cloud service provider agreement, insurance may be a highly attractive addition.[348] So-called "cyber liability insurance"[349] or "cloud insurance," with the potential to provide a more satisfactory third alternative, is becoming increasingly

inevitable,[350] attracting entrepreneurial ventures—such as US-based CloudInsure with customized/tailored insurance solutions[351]—to fill the commercial void.

From the CloudInsure website:

> *Until now, [companies have] mitigated the financial risk of data loss or security intrusion within the Cloud environment … through the reliance on SLA's (Service Level Agreement) credits or a contractual indemnity obligation with their Provider. The first method is ineffective and the second typically requires a trip to the courthouse. Now there is another risk mitigation tool available – one that aligns with the most common mode of economic risk mitigation: Cloud Insurance.*[352]

"Cloud Insurance" for Australian Businesses? – Several Australian insurance companies provide cyber liability insurance (discussed above). However, at present, there exists no comparable cloud insurance for Australian domiciled businesses compensating for lost revenues.

The primary impediments to the development of a domestic cloud insurance are a function of the challenges of developing local risk assessment techniques, the size of the local market, and the entrepreneurial temperament of local insurance providers.

CloudInsure employs a proprietary risk assessment technique based principally on the cloud service provider employed by, and the data risk profile of, the insured.[353] It is unclear if the current local demand for cloud insurance is sufficient to attract the development of home-grown or transplanted and adapted cloud risk assessment techniques. However, as awareness of cloud-related risks increases, so too will the size of the local market for cloud insurance, increasing the commercial attractiveness of developing an Australian species of cloud insurance.

Summary:

- In Australia, it is unlikely that existing cyber liability or business interruption insurance policies will aid any dissatisfied small business users of cloud computing services;
- If the United States is a judicial indicator, there is some sign that business interruption insurance policies relating to suppliers may extend to functional impairment to suppliers' services;
- While existing insurance policies appear deficient and judicial uncertainty prevails, entrepreneurial groups—such as Silicon Valley-based CloudInsure—are moving in to fill the commercial void with customized insurance policies specifically tailored to address the needs of cloud computing customers. It is unclear if current market conditions are sufficient to foster the development of an Australian species of cloud insurance.

10 Small Business & Third Party Technical Consulting Services

In 2003, more than 50% of Australian "small businesses" were non-employing businesses (eg. sole proprietorships) and almost 90% had less than five employees.[354] With so few personnel, small businesses often lack the technical expertise to understand and evaluate relevant cloud computing offerings, and turn to third-party consultants for advice. But what if the consultant's recommendation is poor or inappropriate? What recourse does the small business have?

The prospect of civil proceedings is an anathema to most small businesses. However, consultants employed by small businesses are often small (or relatively small) businesses themselves. Therefore, immediately there is significantly greater equality of bargaining power, opening up greater opportunities for a negotiated outcome – without the need and, more importantly, the associated expense of court proceedings. But on what basis? In short, a small business has potentially three principal causes of action that can form the basis for a negotiated outcome: negligence, breach of contract, and misrepresentation:

(i) ***Negligence*** – The consultant has a duty of care to exercise their professional skills to a reasonable standard based on all the facts available to them. While it is generally acceptable for consultants to make some kind of error, if they provide advice that is simply wrong (based on the facts) and they should have reasonably known the advice was wrong, and the advice costs the business, then the small business has a case for professional negligence.[355] However, there are always complications; (for example) whether the client's expectations changed after the system was established.[356]

(ii) ***Breach of Contract*** – Unlike accountants or lawyers that usually have fiduciary relationships with clients, technical consultants also typically have a contractual relationship.[357] Therefore, a small business may be able to bring an action in both negligence and breach of contract. Consulting contracts may however incorporate limitation of liability clauses serving to protect the consultant against adverse findings – to the extent permitted by State and/or Federal laws.[358]

(iii) ***Misrepresentation*** – There is also the possibility of misrepresentation either at law or in legislation. The small business may have an action if the consultant knowingly or recklessly makes a false or misleading representation to the small business, and the small business relies on the representation causing loss.[359, 360]

Summary – While small business eschews legal proceedings wherever possible, in the context of technical consultants—often themselves small businesses—with greater equality of bargaining power, small business has greater prospects for effecting satisfactory outcomes.

11 Future of Small Business & Cloud service provider Contracts – Still no light at the end of the tunnel for small business

> *It is likely that in the future, cloud computing will [bifurcate]. There will be one market in which services are cheap or free and advertising-supported, and in which the customer takes nearly all the risk. This is the typical model for cloud computing at the moment. But there will also be a market for cloud computing in which the service provider takes more of the risk, in return for more payment.*[361]

As the cloud computing market matures, it is likely that the cloud service provider offerings will diverge into budget versus premium products. Cloud computing is already seeing early evidence of this bifurcation in market offerings, with service providers providing low-cost solutions (ie. the status quo) while others provide more premium services, assuming greater compliance risk and potential liability.[362]

But for small business, there is the very real risk of getting stuck at the wrong end of the deal. In noting the potential bifurcation of cloud offerings, Timothy Callaway alludes to the potential problem:

> *… one set of cloud providers could continue to include limitation on liability clauses and cater to customers who do not store valuable data in the cloud, while the other set could remove the clauses and sell services to those who entrust cloud providers with valuable data.*[363]

Almost invariably, small businesses operate in a highly financially constrained environment – a principal attraction of the cloud for them is cost reduction. Yet they also need to be able to store critical business data in the cloud.

Despite increasing variability in cloud offerings, absent judicial or regulatory intervention, small business is at risk of maintaining the status quo, being wedged unfavourably between consumers—with their consumer protection laws, etc.—and larger organisations—with their much larger technical, legal and financial resources.

12 Conclusion

> *… it is likely that a combination of technical solutions, business practices, and standard contracts between [cloud service providers] and customers will be able to resolve most if not all [cloud computing concerns].*[364]

Compared with larger organisations, small business operates in a distinctive, highly resource constrained operating environment, rendering the promise of cloud computing to smooth cash flows and reduce IT overhead highly attractive.

However, as this report has illustrated, in adopting cloud computing, it is this distinct operating environment that also renders small businesses distinctly vulnerable to criminal, regulatory and legal threats. For example:

- ***Cybercrime*** – While cloud service providers themselves hold much greater appeal to cybercriminals, it is the cloud service provider's small business tenants—experiencing disrupted services and hence disruption to their already fragile revenues—that are the real victims. Lacking policies, procedures and training relating to cyber and network security, small businesses are particularly vulnerable to having account details stolen, and their cloud services hijacked.
- ***Regulation*** – A routine international e-commerce transaction may require a small business to comply with myriad state- and federal-level domestic and international regulations and industry-specific standards. Even storing the business's MYOB files on a cloud storage service (such as Dropbox) may render the small business non-compliant.
- ***Legal*** – Desperate to cut costs, but largely devoid of bargaining power, small businesses are compelled to acquiesce to cloud service agreements often with a choice-of-law in a foreign jurisdiction and limitations of liability so broad as to absolve the cloud service provider of substantially all liability.

For the small business, the promise of cloud computing is great. Conversely, compared with larger corporations, the manifold criminal, regulatory and legal threats can be equally (if not more) devastating. The net result for small business is to transform cloud computing into a form of commercial Russian roulette with its all-or-nothing consequences.

Technical & Commercial Practices to Reduce Risks – There are however technical and commercial practices that can be implemented today by small businesses to reduce at least some of the security and commercial risks:

- *Policies & Training* – Small businesses can provide computer security training to personnel, and institute simple policies setting out (for example) how computer resources should be used, how often passwords should be changed, access rights for staff, and how and when employees may bring in and use their own devices.
- *Industry Education* – Industry bodies can provide education and training to small businesses of appropriate practices and regulatory requirements.
- *Cyber & Cloud Insurance* – Existing cyber liability insurance holds out some, limited hope of compensating for losses as a result of cybercrime. However, the best hope for broader coverage rests with contingent business interruption

insurance adapted to the unique circumstances of cloud computing ("cloud insurance") being developed by entrepreneurial ventures such as CloudInsure.

Opportunities for Legislative Intervention – The near-term future of cloud computing shows signs of bifurcation into budget solutions (much like existing offerings) and premium services with increased security and regulatory compliance, and greater acceptance of liability. But without a change in relative bargaining power between the cloud service provider and small business, it is unclear if competitive forces alone will be sufficient to bring about quality premium services at a price affordable to cost-conscious small business.

To encourage cloud service providers to deliver more attractive, secure and cost effective solutions, inequality of bargaining power between cloud service providers and small business clients will need to be addressed. In this respect, there is significant opportunity for judiciously applied legislative intervention. Opportunities for such carefully considered intervention include: a refined doctrine of unconscionability; possible introduction of legal principles broadly akin to "contracts of adhesion" in the United States; and new regulatory powers—possibly adapted from the ACIF Code—to police the cloud computing industry.

> *I've had too many personal experiences get messed up just because companies change things on the cloud. ... Features change and get dropped, things you depend on disappear, etc. And no company will ever take responsibility. ... Regulation is the only way we'll own a bit of what we trust to the cloud. ... And it would be better for this regulation to begin now, not in 30 years, when it may be too late.*[365]
>
> Steve Wozniak, co-founder Apple (August 2012)

Acting in concert, a combination of technical and commercial solutions—including improved cybersecurity practices, industry education programs, and new species of "cloud insurance"—together with legislative programs may serve to place small business on substantially the same footing as larger businesses, enabling them to fully capture the true benefits of cloud computing while enduring a more equitable share of the risks.

Endnotes

[1] Australian Bureau of Statistics 2001. *Small Business in Australia*. Cat. No. 1321.0. Canberra: ABS http://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/1321.0, retrieved June 20, 2012

[2] Australian Bureau of Statistics 2012. *Counts of Australian businesses, including entries and exits. cat. no. 8165.0*. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0Jun%202007%20to%20Jun%202011?OpenDocument

[3] Welsh, John A. & White, Jerry F., "A small business is not a little big business," *Harvard Business Review* 59(4) (1981) 18-32 at 18.

[4] Welsh *et al*, above note 3 at 32.

[5] Ellis Connolly, David Norman & Tim West, *Small Business: An Economic Overview*, Small Business Finance Round Table, May 2012.

[6] In 2004, almost 35% of full-time small business operators "usually worked" 50+ hours each week, 8127.0, *Characteristics of Small Business, Australia* (Reissue), 2004, Australian Bureau of Statistics, see http://www.abs.gov.au/AUSSTATS/abs@.nsf/0/54B9D7D5493E67B5CA25749C0011424E.

[7] Connolly et al, above note 5.

[8] *Australian Small Business, Key Statistics*, Department of Innovation, Industry, Science and Research, 2011 at 16-19.

[9] Drue Reeves & Daryl Plummer, "The Truth About Cloud Economics" *Harvard Business Review Blog Network*, April 13, 2012, see http://blogs.hbr.org/cs/2012/04/the_truth_about_cloud_economic.html retrieved May 13, 2012.

[10] Securing your start-up or small business, *AVG Australia and New Zealand*, 2010, see http://www.avg.com.au/files/avg/brochures/Securing_Your_Start_Up.pdf, accessed August 23, 2012.

[11] *Small Business Tech Poll 2012*, AT&T, 2012, see http://www.att.com/Common/about_us/files/pdf/national_findings_fact_sheet_wireless.pdf, retrieved August 23, 2012: "Nearly all small businesses (96%) surveyed use wireless technologies [including both mobile and WiFi] in their operations …"

[12] https://www.dropbox.com/plans

[13] https://www.box.com/pricing/

[14] http://www.sugarsync.com/plans/

[15] http://www.salesforce.com/crm/editions-pricing.jsp

[16] http://www.sugarcrm.com/page/editions-pricing/en

[17] http://www.zoho.com/crm/zohocrm-pricing.html

[18] http://www.google.com/enterprise/apps/business/pricing.html

[19] http://www.zoho.com/docs/zoho-docs-pricing.html

[20] http://basecamp.com/pricing

[21] http://teamgantt.com/pricing/

[22] http://asana.com/product#pricing

[23] Freemium, Wikipedia, http://en.wikipedia.org/wiki/Freemium, retrieved July 25, 2012.

[24] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, Anand Ghalsasi, "Cloud computing – The business perspective," *Decision Support Systems* 51 (2011) 176-189 at 184.

[25] Mark Vincent, Nick Hart & Kate Morton, *Cloud Computing Contracts White Paper: A Survey of Terms and Conditions*, Truman Hoyle Lawyers [date?], http://www.itnews.com.au/pdf/Cloud-Computing-Contracts-White-Paper.pdf, retrieved July 7, 2012.

[26] Mark Wittow & David Buller, "Cloud Computing: Emerging legal issues for access to data anywhere, anytime," *Journal of Internet Law*, Volume 14, Number 1, July 2010, 1 at 5.

[27] W. Michael Ryan, Christopher M. Loeffler, "Insights into Cloud Computing," (2010) 22:11 *Intellectual Property & Technology Law Journal* 22.

[28] Miranda Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," (2009) 6:1 *SCRIPTed Journal of Law, Technology and Society* 132.

[29] See for example, Google Apps, Service Level Agreement (SLA) "[Google Apps] will be operational and available to Customer at least 99.9% of the time in any calendar month" at http://www.google.com/apps/intl/en/terms/sla.html, retrieved July 18, 2012.

[30] See for example, The Texas Boot Company among others.

[31] Banham R 2012. Few data breaches in the cloud-for now. *Business Insurance*, 46(3), 14-14.

[32] Banham R 2012. Few data breaches in the cloud-for now. *Business Insurance*, 46(3), 14-14.

[33] Pacella R M 2011. Hacking the cloud. *Popular Science*, *278*(4), 68-71, at 70.

[34] Blumenthal M S 2011. Is Security Lost in the Clouds? *Communications and Strategies*(81), 69-86.

[35] Eddy N 2011. Businesses Face Security Issues With Cloud Service Providers: Report. *Channel Insider*, 1-1; Security Director's Report 2011. Taking it to the Cloud--Can (Should) Security Jump on the Bandwagon? *Security Director's Report*, *11*(8), 2-5; and Trend Micro 2011. *Cloud Security Survey Global Executive Summary*. http://newsroom.trendmicro.com/file.php/194/Global+Cloud+Survey+Exec+Summary_Final+%282%29.pdf

[36] Trend Micro 2011. *Cloud Security Survey Global Executive Summary*. http://newsroom.trendmicro.com/file.php/194/Global+Cloud+Survey+Exec+Summary_Final+%282%29.pdf

[37] Ponemon Institute 2011. *Security of Cloud Computing Providers Study*. Traverse City: Ponemon Institute. http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf; and Security Director's Report 2011. Taking it to the Cloud--Can (Should) Security Jump on the Bandwagon? *Security Director's Report*, *11*(8), 2-5, at 2.

[38] Ponemon Institute 2011. *Security of Cloud Computing Providers Study*. Traverse City: Ponemon Institute. http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf.

[39] Fortify 2010. Vast Scale of Cloud Hacking. *International Journal of Micrographics & Optical Technology*, *28*(3), 7-8, at 7.

[40] Fortify 2010. Vast Scale of Cloud Hacking. *International Journal of Micrographics & Optical Technology*, *28*(3), 7-8.

[41] Dlodlo N 2011. Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing. *Proceedings of the European Conference on Information Management & Evaluation*, 161-168; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *Ieee Security & Privacy*, *9*(2), 50-57.

[42] IT Now 2010. Managing identities. *IT Now*, *52*(2), at 22.

[43] Wright A 2011. Cloud computing and security. *Toledo Business Journal*, *27*(11), 20-22, at 20.

[44] Banks A 2010. Living in the cloud. *APC*, *30*(12), 30-34, at 33.

[45] Banham R 2012. Few data breaches in the cloud-for now. *Business Insurance*, *46*(3), 14-14, at 14.

[46] Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *Ieee Security & Privacy*, *9*(2), 50-57; and Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

[47] Kunick J M 2011. Navigate the cloud. *Managing Intellectual Property*(210), 18, at 18.

[48] Banham R 2012. Few data breaches in the cloud-for now. *Business Insurance*, *46*(3), 14-14, at 14.

[49] Lin P P 2010. SaaS: What Accountants Need to Know. *CPA Journal*, *80*(6), 68-72, at 69.

[50] Agrawal D, El Abbadi A & Wang S 2011. Secure Data Management in the Cloud. *Databases in Networked Information Systems, 7108*, 1-15; American Agent & Broker 2011. Cloud computing creates crime "superhighway". *American Agent & Broker, 83*(2), 10-10; Ang L, Lin G & Kuai X. (2010, 6-10 Dec. 2010). *Fast Anomaly Detection for Large Data Centers.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE; Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400.* Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; Express Computer 2010. Securing the Cloud. *Express Computer*, n/a; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *Ieee Security & Privacy, 9*(2), 50-57; Grosse E, Howie J, Ransome J, Reavis J & Schmidt S 2010. Cloud Computing Roundtable. *Security & Privacy, IEEE, 8*(6), 17-23; Kaufman L M 2010. Can Public-Cloud Security Meet Its Unique Challenges? *Security & Privacy, IEEE, 8*(4), 55-57; Lin P P 2010. SaaS: What Accountants Need to Know. *CPA Journal, 80*(6), 68-72; Pacella R M 2011. Hacking the cloud. *Popular Science, 278*(4), 68-71; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional, 14*(1); and Xu H, Reddyreddy A & Fitch D F 2011. Defending Against XML-Based Attacks Using State-Based XML Firewall. *Journal of Computers, 6*(11).

[51] Pacella R M 2011. Hacking the cloud. *Popular Science, 278*(4), 68-71.

[52] Blanton S & Schiller C 2010. Is There Safety in the Cloud? *EDUCAUSE Quarterly, 33*(2).

[53] Antonopoulos A 2010b. Password cracking in the cloud. *Network World, 27*(22), 17-17; Aron J 2011. Beware of the botcloud. *New Scientist, 210*(2817), 24-24; Biao J, Eul G & Yunmo K 2012. SaaS-Driven Botnets. *Intelligence and Security Informatics. Proceedings Pacific Asia Workshop, PAISI 2012;* Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400.* Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Pacella R M 2011. Hacking the cloud. *Popular Science, 278*(4), 68-71; and, Ren K, Wang C & Wang Q 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing, 16*(1).

[54] Antonopoulos A 2010. Password cracking in the cloud. *Network World, 27*(22), 17-17; Blanton S & Schiller C 2010. Is There Safety in the Cloud? *EDUCAUSE Quarterly, 33*(2); Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400.* Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; Ren K, Wang C & Wang Q 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing, 16*(1).

[55] Hong Kong Government News. (2011). LCQ3 Information security, *Hong Kong Government News*, p. n/a.

[56] Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400.* Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; and, Greene T 2011. Cloud services useful for criminals. *Network World, 28*(2), 16-16.

[57] Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400.* Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx.

[58] Allen J 2010. Data Security in a Mobile World. *GPSolo, 27*(8), 4-6.

[59] Bennett B 2012. Megaupload raid underlines cloud risks. *NZ Business, 26*(2), 54-54, at 54.

[60] ComputerWorld 2010. Collaboration key to privacy in cloud: Minister for Privacy and Freedom of Information. *ComputerWorld*, 3-3.

[61] Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541, at 533.

[62] Abbadi I M 2011. Toward trustworthy clouds' internet scale critical infrastructure. *Information Security Practice and Experience. Proceedings of the 7th International Conference, ISPEC 2011*; Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Antonopoulos A 2010. Cloud security: Root of trust. *Network World, 27*(3), 14-14; Berson S A 2011. Safe in the Cloud? Online Service Risks Need Care and Coverage. *ABA Journal, 97*(11), 22-22; Blumenthal M S 2011. Is Security Lost in the Clouds? *Communications and Strategies*(81), 69-86; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Computer Weekly 2010. Beware the hidden cost of deploying a private cloud. *Computer Weekly*, 12-12; Express Computer 2010. Securing the Cloud. *Express Computer*, n/a; Express Computer 2011. Maintaining security in the Cloud. *Express Computer*, n/a; Ge C & Ohoussou A K. (2010, 25-27 June 2010). *Sealed storage for trusted cloud computing.* Paper presented at the Computer Design and Applications (ICCDA), 2010 International Conference on; Grosse E, Howie J, Ransome J, Reavis J & Schmidt S 2010. Cloud Computing Roundtable. *Security & Privacy, IEEE, 8*(6), 17-23; Khorshed M T, Ali A B M S & Wasimi S A 2011. Trust Issues that Create Threats for Cyber Attacks in Cloud Computing. *Proceedings of the 2011 IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS 2011);* Lin P P 2010. SaaS: What Accountants Need to Know. *CPA Journal, 80*(6), 68-72; McMahon G 2010. Untitled. *Computer Weekly*, 43-43; Ren K, Wang C & Wang Q 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing, 16*(1); Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11; Walters R 2010. Managing privileged user activity in the datacentre. *Network Security, 2010*(11); Yang K, Zhang J, Zhang W & Qiao D 2011. A Light-Weight Solution to Preservation of Access Pattern Privacy in Un-trusted Clouds. *Computer Security - ESORICS 2011. Proceedings 16th European Symposium on Research in Computer Security*.

[63] Blumenthal M S 2010. Hide and Seek in the Cloud. *Security & Privacy, IEEE, 8*(2), 57-58; Computer Weekly 2010. Beware the hidden cost of deploying a private cloud. *Computer Weekly*, 12-12; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *Ieee Security & Privacy, 9*(2), 50-57; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; The Economist. (2010). Cloudy with a chance of rain Tech.view. *Economist.com / News Analysis*, n/a-n/a.

[64] Ang L, Lin G & Kuai X. (2010, 6-10 Dec. 2010). *Fast Anomaly Detection for Large Data Centers.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE; Aron J 2011. Beware of the botcloud. *New Scientist, 210*(2817), 24-24; Biedermann S & Katzenbeisser S 2011. Detecting Computer Worms in the Cloud. *Open Problems in Network Security. IFIP WG 11.4 International Workshop (iNetSec 2011). Revised Selected Papers;* Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400.* Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; ComputerWorld 2010. Collaboration key to privacy in cloud: Minister for Privacy and Freedom of Information. *ComputerWorld*, 3-3; Dlodlo N 2011. Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing. *Proceedings of the European Conference on Information Management & Evaluation*, 161-168; Express Computer 2010b. Securing the Cloud. *Express Computer*, n/a; Ge C & Ohoussou A K. (2010, 25-27 June 2010). *Sealed storage for trusted cloud computing.* Paper presented at the Computer Design and Applications (ICCDA), 2010 International Conference on; Grosse E, Howie J, Ransome J, Reavis J & Schmidt S 2010. Cloud Computing Roundtable. *Security & Privacy, IEEE, 8*(6), 17-23; Journal of E-Governance 2011. Guidelines on Security and Privacy in Public Cloud Computing. *Journal of E-Governance, 34*(3), 149-151; Kaufman L M 2010. Can Public-Cloud Security Meet Its Unique Challenges? *Security & Privacy, IEEE, 8*(4), 55-57; Lin P P 2010. SaaS: What Accountants Need to Know. *CPA Journal, 80*(6), 68-72; North Carolina State University 2010. New research offers security for virtualization, cloud computing. *Computer Weekly News*, 40; Pacella R M 2011. Hacking the cloud. *Popular Science, 278*(4), 68-71; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; Ren K, Wang C & Wang Q 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing, 16*(1); Rubenstein R 2010. Safe sets. *Total Telecom Magazine*, 28-29;

The Economist. (2010). Cloudy with a chance of rain Tech.view. *Economist.com / News Analysis*, n/a-n/a; Thilmany J 2010. Cloud safe. *Mechanical Engineering*, *132*(8), 17-18; Trends Magazine 2011. The Internet Grows More Dangerous. *Trends Magazine*(100), 24-27; and, Zhang Y 2011. Cloud Security. *Technology Review*, *114*(3), 93-93.

[65] Abbadi I M 2011. Toward trustworthy clouds' internet scale critical infrastructure. *Information Security Practice and Experience. Proceedings of the 7th International Conference, ISPEC 2011*; Agrawal D, El Abbadi A & Wang S 2011. Secure Data Management in the Cloud. *Databases in Networked Information Systems*, *7108*, 1-15; Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor*, *68*(4), 35-39; Ang L, Lin G & Kuai X. (2010, 6-10 Dec. 2010). *Fast Anomaly Detection for Large Data Centers.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE; Blumenthal M S 2010. Hide and Seek in the Cloud. *Security & Privacy, IEEE*, *8*(2), 57-58; Blumenthal M S 2011. Is Security Lost in the Clouds? *Communications and Strategies*(81), 69-86; Choo K-K R 2010. *Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal Justice series no. 400*. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; Express Computer 2010b. Securing the Cloud. *Express Computer*, n/a; Express Computer 2011. Maintaining security in the Cloud. *Express Computer*, n/a; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *Ieee Security & Privacy*, *9*(2), 50-57; Khorshed M T, Ali A B M S & Wasimi S A 2011. Trust Issues that Create Threats for Cyber Attacks in Cloud Computing. *Proceedings of the 2011 IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS 2011);* Pacella R M 2011. Hacking the cloud. *Popular Science*, *278*(4), 68-71; Ren K, Wang C & Wang Q 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing*, *16*(1); Ristenpart T, Tromer E, Shacham H & Savage S. (2009). *Hey, you, get off my cloud: Exploring information leakage in third-party compute clouds.* Paper presented at the 16th ACM Conference Computer and Communications Security, Chicago; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional*, *14*(1); and, Zhang Y 2011. Cloud Security. *Technology Review*, *114*(3), 93-93.

[66] Ristenpart T, Tromer E, Shacham H & Savage S. (2009). *Hey, you, get off my cloud: Exploring information leakage in third-party compute clouds.* Paper presented at the 16th ACM Conference Computer and Communications Security, Chicago.

[67] Pacella R M 2011. Hacking the cloud. *Popular Science*, *278*(4), 68-71; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

[68] Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx.

[69] Agrawal D, El Abbadi A & Wang S 2011. Secure Data Management in the Cloud. *Databases in Networked Information Systems*, *7108*, 1-15; Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor*, *68*(4), 35-39; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Express Computer 2010b. Securing the Cloud. *Express Computer*, n/a; McMahon G 2010. Untitled. *Computer Weekly*, 43-43.

[70] Brodkin J 2010. Is Google hack an attack on cloud computing? *Network World (Online)*, n/a.

[71] American Agent & Broker 2011. Cloud computing creates crime "superhighway". *American Agent & Broker*, *83*(2), 10-10; Dlodlo N 2011. Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing. *Proceedings of the European Conference on Information Management & Evaluation*, 161-168; Express Computer 2010. Public, Private or Hybrid? *Express Computer*, n/a; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy*, *9*(2), 50-57; Metzler J & Taylor S 2011. How the network supports cloud computing. *Network World (Online)*, n/a; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business*, *3*(9), 1323-1329; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional*, *14*(1).

[72] Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy, 9*(2), 50-57.

[73] Agrawal D, El Abbadi A & Wang S 2011. Secure Data Management in the Cloud. *Databases in Networked Information Systems, 7108*, 1-15.

[74] Dlodlo N 2011. Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing. *Proceedings of the European Conference on Information Management & Evaluation*, 161-168; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy, 9*(2), 50-57; Metzler J & Taylor S 2011. How the network supports cloud computing. *Network World (Online)*, n/a; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional, 14*(1); Xu H, Reddyreddy A & Fitch D F 2011. Defending Against XML-Based Attacks Using State-Based XML Firewall. *Journal of Computers, 6*(11).

[75] Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

[76] Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy, 9*(2), 50-57.

[77] Dlodlo N 2011. Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing. *Proceedings of the European Conference on Information Management & Evaluation*, 161-168; Grosse E, Howie J, Ransome J, Reavis J & Schmidt S 2010. Cloud Computing Roundtable. *Security & Privacy, IEEE, 8*(6), 17-23; McMahon G 2010. Untitled. *Computer Weekly*, 43-43; Rubenstein R 2010. Safe sets. *Total Telecom Magazine*, 28-29.

[78] Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39.

[79] Brodkin J 2010. Is Google hack an attack on cloud computing? *Network World (Online)*, n/a.

[80] Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx.

[81] Agrawal D, El Abbadi A & Wang S 2011. Secure Data Management in the Cloud. *Databases in Networked Information Systems, 7108*, 1-15; Grosse E, Howie J, Ransome J, Reavis J & Schmidt S 2010. Cloud Computing Roundtable. *Security & Privacy, IEEE, 8*(6), 17-23; Lin P P 2010. SaaS: What Accountants Need to Know. *CPA Journal, 80*(6), 68-72; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional, 14*(1).

[82] Banks L 2010. Cyber criminals using cloud to launch attacks, security expert warns. *ComputerWorld*, 3-3; Journal of E-Governance 2011. Guidelines on Security and Privacy in Public Cloud Computing. *Journal of E-Governance, 34*(3), 149-151; Messmer E 2010. Cloud computing security skeptics abound. *Network World (Online)*, n/a; Rubenstein R 2010. Safe sets. *Total Telecom Magazine*, 28-29.

[83] Financial Express. (2011). In 'smart' era, companies face threat to data security, *Financial Express*, p. n/a; International Rental News 2012. Software in the Cloud. *International Rental News, 12*(1), 26-29; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

[84] Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy, 9*(2), 50-57; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

[85] American Agent & Broker 2011. Cloud computing creates crime "superhighway". *American Agent & Broker, 83*(2), 10-10; Dlodlo N 2011. Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing. *Proceedings of the European Conference on Information Management & Evaluation*, 161-168; Express Computer 2010. Public, Private or Hybrid? *Express Computer*, n/a; Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities.

IEEE Security & Privacy, *9*(2), 50-57; Metzler J & Taylor S 2011. How the network supports cloud computing. *Network World (Online)*, n/a; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business*, *3*(9), 1323-1329; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional*, *14*(1).

[86] Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

[87] Schreiber T 2004. *Session riding: A widespread vulnerability in today's web applications.* Munchen: SecureNet. http://www.securenet.de/papers/Session_Riding.pdf

[88] Grobauer B, Walloschek T & Stoecker E 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy*, *9*(2), 50-57; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business*, *3*(9), 1323-1329; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11; Tsai H-Y, Siebenhaar M, Miede A, Yulun H & Steinmetz R 2012. Threat as a Service?: Virtualization's Impact on Cloud Security. *IT Professional*, *14*(1).

[89] Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business*, *3*(9), 1323-1329; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

[90] Australian Law Reform Commission 2008. *For Your Information: Australian Privacy Law and Practice*. Sydney: Commonwealth of Australia. http://www.alrc.gov.au/publications/report-108

[91] Smith R G. (2002). White collar crime. In A Graycar & P Grabosky (Eds.), Cambridge Handbook of Australian Criminology (pp. 126-156). Melbourne: Cambridge University Press.

[92] Buchanan L. (2008). *Conceal or reveal? Reporting white-collar crime.* Sydney: Clayton Utz. http://www.claytonutz.com/publications/newsletters/litigation_and_dispute_resolution_insights/20080904/conceal_or_reveal_reporting_white-collar_crime.page

[93] Richards K 2009. *The Australian Assessment of Computer User Security: A National Survey*. Canberra: Australian Institute of Criminology.

[94] AusCERT 2006. *Australian 2006 Computer Crime & Security Survey*. Brisbane: AusCERT.

[95] AusCERT 2006. *Australian 2006 Computer Crime & Security Survey*. Brisbane: AusCERT.

[96] Dacosta I, Chakradeo S, Ahamad M & Traynor P 2011. *One-time cookies: Preventing session hijacking attacks with disposable credentials.* Georgia: Georgia Institute of Technology. http://smartech.gatech.edu/handle/1853/37000

[97] Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx

[98] Mansfield-Devine S 2012. Interview: BYOD and the enterprise network. *Computer Fraud & Security*, *2012*(4), 14-17; Thomson G 2012. BYOD: enabling the chaos. *Network Security*, *2012*(2), 5-8.

[99] Wei X, Gomez L, Neamtiu I & Faloutsos M 2012. *Malicious Android applications in the enterprise: What do they do and how do we fix it?* Paper presented at the ICDE Workshop on Secure Data Management on Smartphones and Mobiles.

[100] Leyden J 2005. *Duo charged over DDoS for hire scam*: The Channel. http://www.channelregister.co.uk/2005/03/22/ddos_for_hire_plot_arrests/

[101] Schneier B 2012. *The vulnerabilities market and the future of security*. http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/

[102] Coviello A 2011. *Open letter to RSA customers*: EMC Corporation. http://www.rsa.com/node.aspx?id=3872

[103] Gorman S & Tibken S 2011. *Security 'tokens' take hit*: The Wall Street Journal. http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html

[104] O'Gorman L 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2019-2040.

[105] Australian Bureau of Statistics 2012. *Counts of Australian businesses, including entries and exits. cat. no. 8165.0*. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0Jun%202007%20to%20Jun%202011?OpenDocument

[106] Brad H 2011. Cutting costs for the small end. Security, accessibility under control - cloud computing & mobility: A special report (pp. 2-2): The Australian.

[107] Australian Bureau of Statistics 2012. *Counts of Australian businesses, including entries and exits. cat. no. 8165.0*. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0Jun%202007%20to%20Jun%202011?OpenDocument

[108] Australian Bureau of Statistics 2012. *Counts of Australian businesses, including entries and exits. cat. no. 8165.0*. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0Jun%202007%20to%20Jun%202011?OpenDocument

[109] Office of the Federal Privacy Commissioner 2001. *Guidelines to the National Privacy Principles*. Sydney: Office of the Federal Privacy Commissioner. http://www.privacy.gov.au/law/apply/guidance

[110] Australian Law Reform Commission 2008. *For Your Information: Australian Privacy Law and Practice*. Sydney: Commonwealth of Australia. http://www.alrc.gov.au/publications/report-108

[111] Australian Bureau of Statistics 2012. *Counts of Australian businesses, including entries and exits. cat. no. 8165.0*. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0Jun%202007%20to%20Jun%202011?OpenDocument

[112] Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx; Rubenstein R 2010. Safe sets. *Total Telecom Magazine*, 28-29; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

[113] Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx; Rubenstein R 2010. Safe sets. *Total Telecom Magazine*, 28-29.

[114] Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx; Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; Rubenstein R 2010. Safe sets. *Total Telecom Magazine*, 28-29.

[115] Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads;

[116] Agrawal D, El Abbadi A & Wang S 2011. Secure Data Management in the Cloud. *Databases in Networked Information Systems, 7108*, 1-15; B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud

Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433.* Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; Ren K, Wang C & Wang Q 2012. Security Challenges for the Public Cloud. *IEEE Internet Computing, 16*(1); Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11; Van Till S 2010. Software-as-a-Service for Security -- What to Look for in a Provider. *SDM: Security Distributing & Marketing, 40*(2), 90-90.

117 Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Qaisar S & Khawaja K F 2012. Cloud computing: Networking/security threats and countermeasures. *Interdisciplinary Journal of Contemporary Research in Business, 3*(9), 1323-1329; Wojcik M 2010. Locking the cloud. *Public CIO, 8*(2), 27-30.

118 Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541.

119 Tominaga T 2011. *Standardization works for security regarding the electromagnetic environment.* Paper presented at the Workshop on Cryptographic Hardware and Embedded Systems, Japan.

120 Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541; Van Till S 2010. Software-as-a-Service for Security -- What to Look for in a Provider. *SDM: Security Distributing & Marketing, 40*(2), 90-90; Walters R 2010. Managing privileged user activity in the datacentre. *Network Security, 2010*(11).

121 Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541; Van Till S 2010. Software-as-a-Service for Security -- What to Look for in a Provider. *SDM: Security Distributing & Marketing, 40*(2), 90-90; Walters R 2010. Managing privileged user activity in the datacentre. *Network Security, 2010*(11).

122 Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541; Walters R 2010. Managing privileged user activity in the datacentre. *Network Security, 2010*(11).

123 Knapp K J, Denney G D & Barner M E 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533-541.

124 Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx

125 Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx

126 Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx

127 Mansfield-Devine S 2012. Interview: BYOD and the enterprise network. *Computer Fraud & Security, 2012*(4), 14-17.

128 Hutchings A 2012. *Computer security threats faced by small businesses in Australia. Trends and Issues in Crime and Criminal Justice series no. 433*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.aspx; Wei X, Gomez L, Neamtiu I & Faloutsos M 2012. *Malicious Android applications in the enterprise: What do they do and how do we fix it?* Paper presented at the ICDE Workshop on Secure Data Management on Smartphones and Mobiles.

129 Wojcik M 2010. Locking the cloud. *Public CIO, 8*(2), 27-30.

[130] Richards K 2009. *The Australian Assessment of Computer User Security: A National Survey*. Canberra: Australian Institute of Criminology.

[131] Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Journal of E-Governance 2011. Guidelines on Security and Privacy in Public Cloud Computing. *Journal of E-Governance, 34*(3), 149-151; Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

[132] Ames B & Brown F 2011. AUDITING the cloud. *Internal Auditor, 68*(4), 35-39; Cloud Security Alliance 2010. *Top threats to cloud computing v1.0*: Cloud Security Alliance. https://cloudsecurityalliance.org/research/top-threats/#_downloads; Journal of E-Governance 2011. Guidelines on Security and Privacy in Public Cloud Computing. *Journal of E-Governance, 34*(3), 149-151; Van Till S 2010. Software-as-a-Service for Security -- What to Look for in a Provider. *SDM: Security Distributing & Marketing, 40*(2), 90-90.

[133] Smith R G, Wolanin N & Worthington G 2003. *e-crime solutions and crime displacement. Trends & Issues in Crime and Criminal Justice series no. 243*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/241-260/tandi243.aspx

[134] Smith R G, Wolanin N & Worthington G 2003. *e-crime solutions and crime displacement. Trends & Issues in Crime and Criminal Justice series no. 243*. Canberra: AIC. http://aic.gov.au/publications/current%20series/tandi/241-260/tandi243.aspx

[135] Robert Cringley, "Cloudy with chance of data loss," *I, Cringley*, August 11, 2012, http://www.cringely.com/2012/08/11/cloudy-with-a-chance-of-data-loss/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+ICringely+%28I%2C+Cringely%29, retrieved August 12, 2012.

[136] Ryan *et al*, above note 27.

[137] Ryan *et al*, above note 27.

[138] Daryl Plummer, The Business Landscape of Cloud Computing," *Gartner*, at 31, see http://www.ft.com/cms/5e231aca-a42b-11e1-a701-00144feabdc0.pdf, retrieved August 17, 2012.

[139] Ryan *et al*, above note 27.

[140] See Jerry Norton, "Assessing cloud computing agreements and controls," *WTN News*, December 31, 2009, http://wtnnews.com/articles/6954/, retrieved August 17, 2012; and YouTube video, Douglas W. Barbin, "Cloud Certification: From compliance requirement to competitive differentiator," *Brightline CPAs & Associates, Inc.*, April 20, 2011, http://www.youtube.com/watch?v=wYiFdnZAlNQ, viewed August 17, 2012.

[141] Plummer, above note 138.

[142] Plummer, above note 138.

[143] Charles Oppenheim, Legal issues for information professionals X: Legal issues associated with cloud computing, (2011) 28 *Business Information Review* 25 at 26. See also, Paul Smith, "Security wake-up call for business," *Australian Financial Review*, July 24, 2012 at 24: "… among the concerns of business leaders … a growing number nominate … the security of online data as a big risk."

[144] Ryan *et al*, above note 27.

[145] Schedule 3 (National Privacy Principles), *Privacy Act* 1988 (Cth).

[146] s.6(1), *Privacy Act* 1988 (Cth).

[147] s.6D(1), *Privacy Act* 1988 (Cth).

[148] s.6(1), 6A & 6C, *Privacy Act* 1988 (Cth).

[149] s.6(1), *Privacy Act* 1988 (Cth).

[150] Principle 4.1, Schedule 3 (National Privacy Principles), *Privacy Act* 1988 (Cth).

[151] Office of the Federal Privacy Commissioner, "Guidelines to then National Privacy Principles," September 2001, see http://www.privacy.gov.au/materials/types/download/8774/6582, retrieved July 23, 2012.

[152] Mark Vincent *et al*, above note 25 at 10.

[153] Mark Vincent *et al*, above note 25 at 10.

[154] Mark Vincent *et al*, above note 25 at 10.

[155] FTC Act (1914), 15 USC § 5.

[156] Ryan *et al*, above note 27, *cf.* "the US has no federal data protection law, and only limited laws at a state level," in Charles Oppenheim, Legal issues for information professionals X: Legal issues associated with cloud computing, (2011) 28 *Business Information Review* 25 at 26.

[157] The *Fair and Accurate Credit Transaction Act* of 2003 is an amendment to the *Fair Credit Reporting Act* (FCRA) 15 U.S.C. § 1681.

[158] The security laws, regulations and guidelines directory, *CSO Online, Security and Risk*, November 2, 2010, see http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory, accessed August 17, 2012.

[159] *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act* 2003, see http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf, retrieved August 17, 2012, implementing ss.114 & 325, *Fair and Accurate Credit Transactions Act* of 2003.

[160] see 201 CMR 17, Standards for the Protection of Personal Information of the Residents of the Commonwealth (Massachusetts) (also known as the 'Mass Protection Law'). See also Ryan *et al*, above note 27.

[161] see Chapter 603A, Personal Information Data Privacy Encryption Law (Nebraska), http://www.leg.state.nv.us/nrs/nrs-603a.html, retrieved August 28, 2012.

[162] s.286, *Corporations Act* 2001 (Cth).

[163] s.262A, *Income Tax Assessment Act* 1936 (Cth).

[164] s.107, *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (Cth).

[165] *Taxation Ruling TR 2005/9, Income tax: record keeping – electronic records*, Australian Tax Office, see http://law.ato.gov.au/pdf/pbr/tr2005-009.pdf, retrieved August 15, 2012.

[166] *Taxation Ruling TR 2005/9, Income tax: record keeping – electronic records*, Australian Tax Office, at 3, see http://law.ato.gov.au/pdf/pbr/tr2005-009.pdf, retrieved August 15, 2012.

[167] *Taxation Ruling TR 2005/9, Income tax: record keeping – electronic records*, Australian Tax Office, at 3, see http://law.ato.gov.au/pdf/pbr/tr2005-009.pdf, retrieved August 15, 2012.

[168] s.289, *Corporations Act* 2001 (Cth)

[169] Darren McMahon, *Using MYOB in Dropbox*, Dardee Bookkeeping, November 9, 2011, see http://www.dardee.com.au/using-myob-in-dropbox, retrieved August 15, 2012: Bookkeepers and accountants describe setting up clients' MYOB files in Dropbox, thereby inadvertently storing client financial records in multiple redundant international locations. NB: Dropbox uses Amazon's Simple Storage Service (S3) to store its files, which stores files in multiple redundant international locations. See also, *Want to use Dropbox to replace your USB thumb drive?* EzyLearn, May 25, 2012, see http://ezylearn.com.au/wordpress/2012/05/want-to-use-dropbox-to-replace-your-usb-thumb-drive/, retrieved August 15, 2012.

[170] Mark Vincent *et al*, above note 25 at 9-10.

[171] Mark Vincent *et al*, above note 25 at 10, citing APRA Draft Prudential Standard CPS 231: "Outsourcing" December 2010, http://www.apra.gov.au/Policy/upload/Draft-CPS-231-Outsourcing-for-consultation-Dec-2010.pdf, retrieved March 3, 2010.

[172] The *Gramm-Leach-Bliley Act* (1999) repealed parts of the *Glass-Steagell Act* (1933), removing barriers to permit financial institutions to combine previously distinct banking, investment and insurance services.

[173] see for example, Regulation E, *Electronic Funds Transfer Act*.

[174] GLB Act (1999), 15 USC §§ 6801-6809 and 6821-6827.

[175] see The Gramm-Leach-Bliley Act (GLB Act) of 1999, in The security laws, regulations and guidelines directory, *CSO Online, Security and Risk*, November 2, 2010, see http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory, accessed August 17, 2012.

[176] In 2010, a survey including 1,436 Australian small businesses found that 43% of respondents took orders for products and services online with 53% receiving payments online, *Sensis e-business report: The online experience of small and medium enterprises*. Melbourne: Telstra Corporation Limited, September 2010, see http://about.sensis.com.au/IgnitionSuite/uploads/docs/Sensis%20e-Business%20Report%20September%2010%20FINAL.pdf

[177] see Payment Card Industry Data Security Standard (PCI DSS), in The security laws, regulations and guidelines directory, *CSO Online, Security and Risk*, November 2, 2010, see http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory, accessed August 17, 2012.

[178] Ryan *et al*, above note 27.

[179] Appendix 4: State/territory general medical record retention requirements, "Personally Controlled Electronic Health Record System: Legislation Issues Paper," *Department of Health and Aging, Australian Government*, see http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehrlegals-document-toc~pcehrlegals-document-app04#.UEAFghJ278k, retrieved August 30, 2012.

[180] *Health Insurance Portability and Accountability Act* 1996.

[181] see also, Health Insurance Portability and Accountability Act (HIPAA), in The security laws, regulations and guidelines directory, *CSO Online, Security and Risk*, November 2, 2010, see http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory, accessed August 17, 2012.

[182] See for example, clause 1.1 (Facilities and Data Transfer), Google Apps for Business (Online) Agreement: "As part of providing the Services Google may transfer store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities." http://www.google.com/apps/intl/en/terms/premier_terms.html, retrieved July 23, 2012.

[183] Mark Vincent *et al*, above note 25 at 7.

[184] *National Privacy Principles, Plain English Summary*, Office of the Australian Information Commissioner, http://www.privacy.gov.au/materials/types/law/view/6893 accessed July 18, 2012.

[185] *Privacy Act* 1988 (Cth), National Privacy Provisions, Provision 9.

[186] Ryan *et al*, above note 27. See also, for example, Charles Oppenheim, Legal issues for information professionals X: Legal issues associated with cloud computing, (2011) 28 *Business Information Review* 25 at 26, and Mark Vincent *et al*, above note 25 at 7.

[187] Ryan *et al*, above note 27.

[188] *United States v Philip Morris USA, Inc.*, 327 F.Supp 2d 21 & 26. Court imposed a fine of $2.7 million against Philip Morris.

[189] see also, Judah Lifshitz and Laura Fraher, "Technology: Corporations take risks by bringing e-discovery in-house," *Inside Counsel*, August 17, 2012, http://www.insidecounsel.com/2012/08/17/technology-corporations-take-risks-by-bringing-e-d , retrieved August 18, 2012, subtitled "If a court orders further search and collection efforts, your e-discovery costs could sour" and citing *National Day Laborer Organizing Network v. United States Immigration and Customs Enforcement Agency*, 2011 WL 381625 (S.D.N.Y. Feb. 7, 2011).

[190] see Federal Rules of Civil Procedure (FRCP), in The security laws, regulations and guidelines directory, *CSO Online, Security and Risk*, November 2, 2010, see http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory, accessed August 17, 2012, citing Rule 26(a), 26(b)(2), 26(f), 33(d), 34(b) and 37(f).

[191] Timothy J. Calloway, "Cloud computing, clickwrap agreements, and limitations on liability clauses: A perfect storm?" (2012) 11 *Duke Law & Technology Review* 163 at 172.

[192] Mark Vincent *et al*, above note 25 at 4.

[193] Calloway, above note 191, citing *Arthur Miller Dance Studios of Cleveland, Inc., v Witter*, 105 N.E.2d 685 at 704 (Ohio Ct. Com. Pl. 1952).

[194] Dale Clapperton & Stephen Corones, "Unfair terms in 'clickwrap' and other electronic contracts," 25 *Australian Business Law Review* 152.

[195] Frank Zumbo, "Dealing with unfair terms in consumer contracts: Is Australia falling behind?" (2005) 13 *TPLJ* 70, at 74.

[196] Ryan *et al*, above note 27.

[197] Wayne Jansen & Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144," *National Institute of Standards and Technology*, December 2011, at vii: "Non-negotiable service agreements in which the terms of service are prescribed completely by the cloud provider are generally the norm in public cloud computing."

[198] Simon Bradshaw, Christopher Millard & Ian Walden, *Contracts and the Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Centre for Commercial Law Studies, Queen Mary, University of London, 2010 at 18.

[199] See for example Google Apps, clause 13.10 (Governing Law): "This Agreement is governed by California law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA." http://www.google.com/apps/intl/en/terms/standard_terms.html, retrieved July 18, 2012.

[200] Mark Vincent *et al*, above note 25 at 4-5.

[201] clause 13.1 (Who you are contracting with, notices, governing law and jurisdiction), Salesforce.com Master Subscription Agreement, see http://www.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf , retrieved July 10, 2012.

[202] Patrick Van Ecke, *Cloud Computing Legal Issues*, DLA Piper, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf, retrieved June 20, 2012.

[203] Mark A. Lemley, "Terms of Use," (2006) 91 *Minnesota Law Review* 459 at 463, see footnote 8.

[204] Lemley, above note 203 at 476, see footnote 61, giving *inter alia* the example of an electronic arbitration clause found unconscionable in *Comb v PayPal, Inc.* 218 F.Supp. 2d 1165 at 1177 (ND Cal. 2002). See also, Richard G. Kundel, "Recent developments in shrinkwrap, clickwrap and browsewrap licenses in the United States," *Murdoch University Electronic Journal of Law*, Volume 9, Number 3, September 2002, citing *Williams v America Online, Inc.*, 43 UCC Rep. Serv. 2d (Callaghan) 1101 (Mass. Super. Ct., February 8, 2001).

[205] *Feldman v Google, Inc.*, 513 F.Supp.2d 229 (ED Pa. 2007).

[206] *In re RealNetworks, Inc. Privacy Litigation*, No. 00-1366, 2000 WL 631341 (D. Ill. May 8, 2000).

[207] Kaustuv M. Das, "Forum-selection clauses in consumer clickwrap and browsewrap agreements and the 'reasonably communicated' test," 77 *Washington Law Review* 481 (2002) at 500, footnote 179.

[208] Calloway, above note 191 at 163.

[209] Catharine Smith, "7,500 online shoppers accidentally sold their souls to GameStation," *Huffington Post*, June 17, 2010, see http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-on_541549.html, retrieved August 20, 2012, and cited by Timothy J. Calloway, "Cloud computing, clickwrap agreements, and limitations on liability clauses: A perfect storm?" (2012) 11 *Duke Law & Technology Review* 163 at 163-64.

[210] Catharine Smith, "7,500 online shoppers accidentally sold their souls to GameStation," *Huffington Post*, June 17, 2010, see http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html, retrieved August 20, 2012, and cited by Calloway, above note 191 at 163-64.

[211] Calloway, above note 191 at 165.

[212] Patrick Van Ecke, *Cloud Computing Legal Issues*, DLA Piper, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf, retrieved June 20, 2012.

[213] For cloud service providers, "direct liability" typically means vendor liability for losses to the customer relating to the loss, damage or otherwise of data hosted on the cloud service, see Bradshaw *et al*, above note 198 at 33.

[214] Calloway, above note 191, see footnote 9.

[215] *ProCD Inc v Zeidenburg*, 86 F.3d 1447 (7th Cir. 1996).

[216] Lemley, above note 203 at 468.

[217] Contracts of adhesion are "standard form contracts presented on a take-it-or-leave-it basis," Todd D. Rakoff, "Contracts of adhesion: An essay in reconstruction," 96 *Harvard Law Review* 1173 (1983). In discussing standard contracts as frequently being contracts of adhesion: "Standard contracts are typically used by enterprises with strong bargaining power. The weaker party, in need of the goods or services, is frequently not in a position to shop around for better terms, either because the author of the standard contract has a monopoly … or because all competitors the same clauses. His contractual intention is but a subjection more or less voluntary to terms dictated by the stronger party, terms whose consequences are often understood only in a vague way, it at all." Friedrich Kessler, "Contracts of Adhesion—Some Thoughts about Freedom of Contract," 43 *Columbia Law Review* 629 (1943) at 632.

[218] see for example: *Step-saver Data Sys., Inc. v Wyse Tech.*, 939 F.2d 91 (3d Cir. 1991), and *Foresight Res. Corp. v Pfortmiller*, 719 F. Supp. 1006.

[219] Timothy J. Calloway, "Cloud computing, clickwrap agreements, and limitations on liability clauses: A perfect storm?" (2012) 11 *Duke Law & Technology Review* 163 at 165, and 169, citing *Trieber & Straub, Inc. v United Parcel Service, Inc.*, No. 04-C-0069, 2005 WL 2108081 (ED Wis., August 31, 2005).

[220] Calloway, above note 191, see footnote 10, quoting Nathan J Davis, Note, Presumed Assent: The Judicial Acceptance of Clickwrap, 22 *Berkley Technology Law Journal*, 577 (2007) at 579. For an example of enforcing a click-wrap agreement, see *Conference America Inc. v Conexant Syst. Inc.*, MD Ala, No. 2:05-cv-01088, September 10, 2007. For an example of enforcement a click-wrap agreement without reading terms, see *Druyan v Jagger*, 508 F.Supp. 2d 228 (SDNY, August 29, 2007).

[221] ss.3 & 64A(2), Schedule 2, *Competition & Consumer Act* 2010 (Cth).

[222] s.60, Schedule 2, *Competition & Consumer Act* 2010 (Cth).

[223] s.61(1), Schedule 2, *Competition & Consumer Act* 2010 (Cth).

[224] s.64A(2), Schedule 2, *Competition & Consumer Act* 2010 (Cth).

[225] see https://www.dropbox.com/pricing, retrieved July 25, 2012.

[226] see http://basecamp.com/pricing, retrieved July 25, 2012.

[227] see http://www.salesforce.com/crm/editions-pricing.jsp, retrieved July 25, 2012.

[228] *Kingsway Hall Hotel Ltd v Red Sky IT (Houslow) Ltd* [2010] EWHC 965.

[229] Above note 228 at para 258.

[230] *GB Gas Holdings v Accenture* [2009] EWHC 2966, upheld in [2010] EWCA Civ 912.

[231] Bradshaw *et al*, above note 198 at 35-36.

[232] *Unconscionability* is a term used in contract law. A contract may be declared unconscionable and therefore voidable if (i) one party was at a "serious disadvantage" (such as illiteracy or a lack of

education) vis-à-vis the other, stronger party, and (ii) the stronger party was aware of the serious disadvantage at the time of forming the contract (see, for example, *Commercial Bank of Australia Limited v Amadio* (1983) 151 CLR 447).

233 Calloway, above note 191 at 174.

234 Calloway, above note 191 at 174.

235 Clapperton *et al*, above note 194 at ???, highlighting that the elements of procedural unconscionability (ie. special disadvantage beyond "mere imbalance of bargaining power"; knowledge of special disadvantage; exploitation of special disadvantage, as set out in *Commercial Bank of Australia v Amadio* (1983) 151 CLR 447) are unlikely to be made out for click-wrap agreements.

236 Clapperton *et al*, above note 194 at ???, citing *Tri-Global (Aust) Pty Limited v Colonial Mutual Life Assurance Society Limited* (1992) ATPR 41-174.

237 see for example *Comb v PayPal, Inc.* 218 F.Supp. 2d 1165 at 1177 (ND Cal. 2002), where court found a clause re arbitration unconscionable. See also, Mark A. Lemley, "Terms of Use," (2006) 91 *Minnesota Law Review* 459 at 463, see footnote 62.

238 Clapperton *et al*, above note 194, citing Zumbo F., "Dealing with Unfair Terms in Consumer Contracts: Is Australia Falling Behind?" (2005) 12 *TPLJ* 70. In comparison, however, see Kirby J's dissenting opinion in *Australian Competition and Consumer Commission v CG Berbatis Holdings Pty Ltd* (2003) 214 CLR 51 at 84, indicating that "the reach of [s.51AA, *Trade Practices Act* (the predecessor to the *Competition and Consumer Act*)], in my view, goes further." See also, J.G. Starke QC, N.C. Seddon & M.P. Ellinghaus, *Cheshire & Fifoot's Law of Contract*, 6th Ed., Butterworths, 1992, at 429 [832]: "Section 52A(2) sets out guidelines as to what is unconscionable and, in doing so, traverses both 'procedural' … and 'substantive' … unconscionability,"

239 Associate Professor, School of Business and Taxation, University of New South Wales.

240 Zumbo, above note 195 at 70 (abstract).

241 see for example: *Oceanic Sun Line Special Shipping Co Inc v Fay* (1988) 165 CLR 197, and *Baltic Shipping Co v Dillon* (1993) 176 CLR 344.

242 Referring to a condition purporting to exclude all liability, "it is so wide and so destructive of rights that the court should not hold any man bound by it unless it is drawn to his attention in the most explicit way. … In order to give sufficient notice, it would need to be printed in red ink with a red hand pointing to it - or something equally startling," *Thornton v Shoe Lane Parking Ltd* [1971] 2 QB 163 *per* Lord Denning MR.

243 Zumbo, above note 195 at 75.

244 see for example, Dale Clapperton & Stephen Corones, "Unfair terms in 'clickwrap' and other electronic contracts," 25 *Australian Business Law Review* 152 at ???, drawing on Frank Zumbo, "Dealing with unfair terms in consumer contracts: Is Australia falling behind?" (2005) 13 *TPLJ* 70, particularly 85-89.

245 ACIF Code, see http://www.acma.gov.au/webwr/telcomm/industry_codes/codes/c620.pdf, retrieved August 1, 2012. Note: The ACIF Code in turn draws heavily from *Fair Trading Act* 1999 (Vic).

246 Clapperton *et al*, above note 194.

247 Clapperton *et al*, above note 194.

248 Above note 245, s.2.2 (Objectives).

249 Above note 245, s.6.1 (Terms must not be unfair).

250 Above note 245, s.4.2 (Definitions).

251 Above note 245, s.6.2 (Assessment of Terms of Unfairness).

252 ss.121(1), (2) & (4), and s.570, *Telecommunications Act* 1997 (Cth). See also, Dale Clapperton & Stephen Corones, "Unfair terms in 'clickwrap' and other electronic contracts," 25 *Australian Business Law Review* 152 at ???.

253 Mark Vincent *et al*, above note 25 at 11.

[254] Zoho, Terms of Service, Disclaimer of Warranties, see http://www/zoho.com/terms.html, retrieved July 18, 2012.

[255] s.18, Schedule 2, *Competition and Consumer Act* 2010 (Cth).

[256] Mark Vincent *et al*, above note 25 at 12.

[257] *The basics in communications needs: Small Business*, AT&T, 2012, at 5, see http://www.att.com/Common/merger/files/pdf/Telecommunications_Basics.pdf, retrieved August 23, 2012.

[258] "Service credits" means (eg) the number of "days of service added to the end of the Service term (or monetary credit equal to the value of the days of service …), at no charge to Customer." See *Google Apps Service Level Agreement*, see http://www.google.com/apps/intl/en/terms/sla.html, retrieved July 23, 20102.

[259] Google Apps SLA clause, *Google Apps Service Level Agreement*, see http://www.google.com/apps/intl/en/terms/sla.html, retrieved July 23, 20102. NB: Under the *Google Apps Service Level Agreement*, the "aggregate maximum number of service credits … issued … in a single calendar month shall not exceed fifteen days."

[260] See for example, Modifications to the Service and Prices, Basecamp Terms of Service, http://basecamp.com/terms, retrieved July 25, 2012: sub-clause 1, "37signals reserves the right at any time and from time to time to modify or discontinue, temporarily or permanently, the Service (of part thereof) with or without notice," and sub-clause 2, "37signals shall not be liable to you or to any third party for any modification, price change, suspension or discontinuance of the Service."

[261] Customer Must Request Service Credit clause, *Google Apps Service Level Agreement*, see http://www.google.com/apps/intl/en/terms/sla.html, retrieved July 23, 20102.

[262] Mark Vincent *et al*, above note 25 at 14.

[263] Mark Vincent *et al*, above note 25 at 6, provide examples of clauses of: (i) unilateral variation, (ii) limited situation variation, and (iii) variation by mutual agreement.

[264] Mark Vincent *et al*, above note 25 at 6.

[265] Mark Wittow & David Buller, "Cloud Computing: Emerging legal issues for access to data anywhere, anytime," *Journal of Internet Law*, Volume 14, Number 1, July 2010, 1 at 5.

[266] USA PATRIOT Act (the Patriot Act) may permit United States-based law enforcement agencies to compel production of information stored in the United States and/or from United States companies with data centres outside the United States.

[267] Patriot Act, *Wikipedia*, http://en.wikipedia.org/wiki/Patriot_Act, retrieved July 27, 2012, quoting the *Electronic Frontiers Foundation* (EFF), "Let the Sun Set on PATRIOT – Section 220: 'Nationwide Service of Search Warrants for Electronic Evidence'" October 12, 2007.

[268] Bradshaw *et al*, above note 198 at 28.

[269] clause 3.2 (Data Privacy), Security and Data Privacy, AWS Customer Agreement, Amazon, http://aws.amazon.com/agreement/, retrieved July 26, 2012.

[270] see ss.215 & 505, USA PATRIOT Act (the Patriot Act) for potential examples.

[271] clause 8.3 (Compelled Disclosure), Master Subscription Agreement, Salesforce, http://www.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf, retrieved July 26, 2012.

[272] clause Compliance with Laws and Law Enforcement Requests; Protection of Dropbox's Rights, Dropbox Privacy Policy, https://www.dropbox.com/pricing_terms#privacy, retrieved July 26, 2012.

[273] clause 1.1 (Facilities and Data Transfer), Services, Google Apps for Business (Online) Agreement, http://www.google.com/apps/intl/en/terms/premier_terms.html, retrieved July 27, 2012.

[274] Bradshaw *et al*, above note 198 at 29.

[275] Bradshaw *et al*, above note 198 at 29.

[276] Mowbray, above note 28 at 12, citing D. Raywood, "Google admits that some of its Docs have been accidentally shared" (2009) *SC Magazine*, 10 March 2009, available at

http://www.scmagazineuk.com/google-admits-that-some-of-itsdocs-have-been-accidentally-shared/article/128491/ (accessed 13 July 2010).

277 Founded in 1999, SalesForce.com is "best known for its on-demand Customer Relationship Management (CRM) solutions," http://www.crunchbase.com/company/salesforce, retrieved July 13, 2012.

278 For an indication: In 2012, SalesForce.com had estimated revenues of US$2.26 billion and employed over 8,300 personnel (http://en.wikipedia.org/wiki/Salesforce.com, retrieved July 13, 2012).

279 Charles Oppenheim, Legal issues for information professionals X: Legal issues associated with cloud computing, (2011) 28 *Business Information Review* 25 at 26. See also, Paul Smith, "Security wake-up call for business," *Australian Financial Review*, July 24, 2012 at 24: "… among the concerns of business leaders … a growing number nominate … the security of online data as a big risk."

280 Ryan *et al*, above note 27.

281 Secure Storage, Security Overview, Dropbox, https://www.dropbox.com/dmca#security, retrieved July 30, 2012.

282 see Terms of Service, Dropbox, https://www.dropbox.com/dmca#terms, retrieved July 30, 2012.

283 see Privacy Policy, Dropbox, https://www.dropbox.com/dmca#privacy, retrieved July 30, 2012.

284 Security Statement, Salesforce, http://www.salesforce.com/au/company/privacy/security.jsp, retrieved July 30, 2012.

285 see Master Subscription Agreement, Salesforce, http://www.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf, retrieved July 30, 2012.

286 clause 1.1 (Facilities and Data Transfer), Services, Google Apps for Business (Online) Agreement, http://www.google.com/apps/intl/en/terms/premier_terms.html, retrieved July 27, 2012.

287 Mark Wittow & David Buller, "Cloud Computing: Emerging legal issues for access to data anywhere, anytime," *Journal of Internet Law*, Volume 14, Number 1, July 2010, 1 at 6.

288 Bradshaw *et al*, above note 198 at 21.

289 Mark Vincent *et al*, above note 25 at 11.

290 See also, Bradshaw *et al*, above note 198 at 22: "In effect, a number of providers of consumer-oriented Cloud services appear to disclaim the specific fitness of their services for the purpose(s) for which many customers will have specifically signed up to use them."

291 Where does Dropbox store everyone's data?, Dropbox, https://www.dropbox.com/help/7/en, retrieved July 24, 2012.

292 Mowbray, above note 28 at 10.

293 Mowbray, above note 28 at 13.

294 clause Your Stuff & Your Privacy, Dropbox Terms of Service, see https://www.dropbox.com/pricing_terms#terms, retrieved July 26, 2012.

295 Memorandum in Support of Non-Party Twitter, Inc.'s Motion to Quash § 2703(d) Order, *Twitter*, http://www.aclu.org/files/assets/memoinsupportofnon-partytwittermotion_to_quash.pdf See also Adam Gabbatt, Twitter sides with Occupy protester in NY court battle over tweet history, *The Guardian (Online)*, May 8, 2012, http://www.guardian.co.uk/technology/2012/may/08/twitter-occupy-new-york-court, retrieved August 6, 2012.

296 Bradshaw *et al*, above note 198 at 31.

297 Mowbray, above note 28 at 11, citing M. Crandell, "RightScale: the cloud management platform" (2009) *Powered by Cloud*, London, 2-3 February 2009, cf. Joe McKendrick, "Cloud computing simply isn't that scary anymore: Survey," *Forbes.com*, June 20, 2012, http://www.forbes.com/sites/joemckendrick/2012/06/20/cloud-computing-simply-isnt-that-scary-anymore-survey/, retrieved July 25, 2012.

[298] Patrick Van Ecke, *Cloud Computing Legal Issues*, DLA Piper, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf, retrieved June 20, 2012.

[299] Mark Vincent *et al*, above note 25 at 14.

[300] clause 11.2 (Effects of Termination), Google Apps for Business (Online) Agreement, http://www.google.com/apps/intl/en/terms/premier_terms.html, retrieved July 23, 2012.

[301] Cancellation and Termination, Basecamp Terms of Service, http://basecamp.com/terms, retrieved July 25, 2012.

[302] clause 12.5 (Return of Your Data), SalesForce.com, Master Subscription Agreement, http://www.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf, retrieved July 10, 2012.

[303] Patrick Van Ecke, *Cloud Computing Legal Issues*, DLA Piper, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf, retrieved June 20, 2012.

[304] Mark Vincent *et al*, above note 25 at 14-15.

[305] Ryan *et al*, above note 27.

[306] Bradshaw *et al*, above note 198 at 23.

[307] clause 7.3 (Effect of Termination), AWS Customer Agreement, Amazon Web Services, see http://aws.amazon.com/agreement/, retrieved July 26, 2012. Similarly, see clause 5 (Data Retention), Dropbox Privacy Policy, see https://www.dropbox.com/pricing_terms#privacy, retrieved July 25, 2012.

[308] "after a commercially reasonable period of time, Google will delete Customer Data," clause 11.2 (Effects of Termination), Google Apps for Business (Online) Agreement, http://www.google.com/apps/intl/en/terms/premier_terms.html, retrieved July 23, 2012; and "After such 30-day period, We shall … unless legally prohibited, delete all of Your Data in Our systems," clause 12.5 (Return of Your Data), SalesForce.com, Master Subscription Agreement, http://www.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf, retrieved July 10, 2012.

[309] Bradshaw *et al*, above note 198 at 25.

[310] Terms & Conditions, 3Tera, see http://www.3tera.com/Terms/index.php

[311] Bradshaw *et al*, above note 198 at 23.

[312] *The basics in communications needs: Small Business*, AT&T, 2012, at 5, see http://www.att.com/Common/merger/files/pdf/Telecommunications_Basics.pdf, retrieved August 23, 2012.

[313] Ryan *et al*, above note 27 at 25.

[314] Robert Cringley, "Cloudy with chance of data loss," *I, Cringley*, August 11, 2012, http://www.cringely.com/2012/08/11/cloudy-with-a-chance-of-data-loss/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+ICringely+%28I%2C+Cringely%29, retrieved August 12, 2012.

[315] Ryan *et al*, above note 27 at 25.

[316] see for example, Terms of Service (https://www.dropbox.com/dmca#terms) & Security Overview (https://www.dropbox.com/dmca#security), Dropbox, both retrieved July 30, 2012.

[317] clause 4.2 (Our Protection of Your Data), Master Subscription Agreement, Salesforce, see http://www.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf, retrieved July 30, 2012.

[318] clause 1.1 (Facilities and Data Transfer), Services, Google Apps for Business (Online) Agreement, Google, http://www.google.com/apps/intl/en/terms/standard_terms.html, retrieved July 30, 2012.

[319] Calloway, above note 191 at 170, quoting Daniel Eran Dilger, Microsoft's Danger Sidekick Data Loss Casts Dark on Cloud Computing, *AppleInsider*, October 11, 2009, http://www.appleinsider.com/articles/09/10/11/microsofts_danger_sidekick_data_loss_casts_dark_on_cloud_computing.html

[320] see also ???

[321] *Insights: Data Protection and the Cloud*, Computer Associates, May 2012, at 4, http://www.arcserve.com/us/lpg/~/media/Files/SupportingPieces/ARCserve/Insights-Data-Protection-and-the-Cloud.pdf, retrieved August 6, 2012.

[322] Mowbray, above note 28 at 13.

[323] Calloway, above note 191 at 163.

[324] Freemium, Wikipedia, http://en.wikipedia.org/wiki/Freemium, retrieved July 25, 2012.

[325] Bradshaw *et al*, above note 198 at 15.

[326] Free Accounts, Dropbox Pricing Terms and Conditions, https://www.dropbox.com/pricing_terms, retrieved July 25, 2012.

[327] See above note 326, "... if a Free Account is inactive for ninety (90) days, then Dropbox may delete any or all of Your Files without providing additional notice."

[328] Ryan Nichols, *CIO's Guide to Cloud Computing and On-Demand*, September 10, 2009, http://blog.appirio.com/2009/09/cloud-insurance.html

[329] Lon Berk, "CBI for the Cloud," *American Bar Association Committee on Insurance Litigation Coverage Letter*, Vol. 21, No. 6, http://www.huntonprivacyblog.com/wp-content/uploads/2012/03/CBI_for_the_Cloud.pdf, retrieved August 1, 2012.

[330] see for example, Policy Section 2: Business interruption, GIO Business Insurance PDS, at 56.

[331] Policy Section 9: Equipment breakdown, GIO Business Insurance PDS, at 115.

[332] *cf*. there is the remote (and extreme?) possibility that the manner and form of the insured's use of cloud provider's servers might render the server/server applications and/or data as the insured's property, see Berk, above note 329 at 3-4, citing *Zurich American Insurance Co. v ABM Industries, Inc.*, 397 F.3d 158 (2d Cir. 2005).

[333] Berk, above note 329 at 3.

[334] Endorsement Code SPREMXB4, Specified Suppliers' and/or Customers' Premises, *Part B: Chapter 1 – Endorsements, Understanding the ISR Policy, Volume 1: Mark IV Advisory & Mark IV Modified*, Chubb Insurance, at 465, received via email, August 9, 2012.

[335] see also, Berk, above note 329 at 3.

[336] Berk, above note 329 at 3.

[337] see also Paul Wordley & Graham Denny, "Business Interruption Insurance: The importance of understanding the cover," *The In-House Lawyer*, January 2011, defining supplier-related business interruption insurance as intended to compensate for (eg) lost income "as a result of physical damage to insured property or other key external events, *such as damage at a supplier's or customer's premises.*" (emphasis added)

[338] see for example, Anthony Wing Kosner, "Amazon cloud goes down Friday night, taking Netflix, Instagram and Pinterest with it," *Forbes*, June 30, 2012, see http://www.forbes.com/sites/anthonykosner/2012/06/30/amazon-cloud-goes-down-friday-night-taking-netflix-instagram-and-pinterest-with-it/, retrieved August 9, 2012.

[339] see for example, Brid-Aine Parnell, "Microsoft's Azure cloud down and out for 8 hours," *The Register*, February 29, 2012, see http://www.theregister.co.uk/2012/02/29/windows_azure_outage/, retrieved August 9, 2012.

[340] Jess B. Millikan, "One Court, Two Decisions: The debate continues as to what constitutes 'direct physical loss' under business interruption insurance," *Bullivant Houser Bailey PC*, January 2007, see http://www.bullivant.com/One-Court-Two-Decisions-The-Debate-Continues, retrieved August 8, 2012.

[341] see Berk, above note 329 at 4 & 5, and citing *America Online, Inc. v St. Paul Mercury Ins. Co.*, 207 F.Supp. 2d 459 (E.D. Va 2002), and *Ward General Ins. Services, Inc. v Employers Fire Ins. Co.*, 7 Cal. Rptr. 3d 844 (Cal. Ct. App. 2004).

[342] *American Guarantee & Liability Ins. Co. v Ingram Micro, Inc.*, 2000 US Dist.2000 WL 726789 (D.Ariz. April 18, 2000).

[343] Above note 342 at 2.

[344] *Southeast Mental Health Center, Inc. v Pacific Ins. Co Ltd.*, 439 F.Supp.2d 831 (WD Tenn. 2006) at 837-38.

[345] *Wakefern Food Corporation v Liberty Mut. Fire Ins. Co.*, 968 A.2d 724 (NJ Super Ct, Div 2009).

[346] Above note 345 at 736.

[347] Berk, above note 329 at 9, also citing *Wakefern Food Corporation v Liberty Mut. Fire Ins. Co.*, 968 A.2d 724 (NJ Super Ct, Div 2009).

[348] Laurin Mills, *Legal Issues Associated with Cloud Computing*, Nixon Peabody, May 13, 2009, see http://www.actgov.org/knowledgebank/documentsandpresentations/Documents/Shared%20Interest%20Groups/Cybersecurity%20SIG/Legal%20Issues%20Associated%20with%20Cloud%20Computing%20-%20Laurin%20Mills%20-%20Nixon%20Peabody%20LLP%20-%2005-13-09.pdf, retrieved July 30, 2012.

[349] Timothy Chou, "The Increasing Inevitability of Cyber Insurance," *CFO.com*, June 12, 2012, http://www3.cfo.com/article/2012/6/it-value_cyber-insurance-technology-risks-cfos, retrieved August 7, 2012.

[350] Chou, above note 349.

[351] see www.cloudinsure.com, founded in June 2010.

[352] see http://www.cloudinsure.com/why_cloudinsure/, retrieved August 1, 2012.

[353] *Ibid*.

[354] 8127.0, Characteristics of Small Business, Australia (Reissue), 2004, *Australian Bureau of Statistics*, http://www.abs.gov.au/AUSSTATS/abs@.nsf/0/54B9D7D5493E67B5CA25749C0011424E.

[355] Tim Bishop, Making a Professional Negligence Claim: Consultants, http://articles.submityourarticle.com/making-a-professional-negligence-claim-consultants-165867, retrieved August 8, 2012.

[356] Gordon Hughes, "Professional Liability: Why computer consultants are different," *Australian Accountant*, October 1988, at 80.

[357] Hughes, above note 356 at 82.

[358] Hughes, above note 356 at 82.

[359] Hughes, above note 356 at 84.

[360] see *Competition and Consumer Act* 2010 (Cth).

[361] Mowbray, above note 28 at 8.

[362] see for example, cloud storage vendors, Egnyte (http://www.egnyte.com/) and Connectria (https://www.connectria.com/), openly promoting their services as HIPAA and EU-US Safe Harbor compliant.

[363] Calloway, above note 191 at 174.

[364] Mowbray, above note 28 at 14.

[365] Steve Wozniak, "Why the cloud sucks," *Gizomodo*, August 6, 2012, see http://gizmodo.com/5932161/why-the-cloud-sucks/, retrieved August 28, 2012.