September 20, 2013

Navigating Through the Fog of Cloud Computing Contracts

T. Noble Foster, *Seattle University*

Navigating Through the Fog of Cloud Computing Contracts

Abstract

This paper explores legal issues associated with cloud computing, provides analysis and commentary on typical clauses found in contracts offered by well-known cloud service providers, and identifies strategies to mitigate the risk of exposure to cloud-based legal claims in the critical areas of data security, privacy, and confidentiality. While current research offers numerous case studies, viewpoints, and technical descriptions of cloud processes, our research provides a close examination of the language used in cloud contract terms. Analysis of these contract terms supports the finding that most standard cloud computing contracts are unevenly balanced in favor of the cloud service provider. The implication for cloud users is that additional measures, both legal and practical, are necessary in order to achieve a reasonable level of data security, privacy, and confidentiality, and to mitigate the inherent risks in cloud computing solutions. Our research was limited to an analysis of some of the leading cloud computing service providers and the contract clauses they offer to cloud users. Although the selected cloud provider contracts are representative of the currently available contract terms throughout the industry, these terms are evolving along with the practices of the cloud providers and cloud users.

Keywords: cloud computing, legal issues, cloud provider contracts, risk, data security

NAVIGATING THROUGH THE FOG OF CLOUD COMPUTING CONTRACTS

Larry Ellison, the famous CEO of Oracle is quoted as stating, "We've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements."[1]

The National Institute of Standards and Technology (NIST) published this concise definition of cloud computing:

> "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, software applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[2]

Cloud computing can take one of several different forms. The NIST identifies four "deployment models" as Private, Community, Public, and Hybrid Clouds.[3]

According to a recent survey of two hundred IT professionals concerning the various deployment models listed above, 51 percent indicated that the most used or likely to be used model is the private cloud, followed by the hybrid model (31 percent) and the public cloud model (11 percent).[4]

Of these four different deployment models, our primary research interest here relates to the Public Cloud model. For our purposes, the other two (Hybrid and Community), are considered to be variations on the same theme and a Private Cloud is a privately owned and controlled data center.

Cloud computing offers scalability, significant cost efficiencies, and 24/7 accessibility. In cloud computing, some or nearly all of an organization's computing resources are "rented" from an external cloud provider on a scalable, pay-per-use or subscription basis Simply put, cloud computing can help organizations reduce costs since they do not have to invest in hardware and other physical infrastructure, nor pay fees for on-going maintenance and upgrades.

---

[1] Farber, D. "Oracle's Ellison nails cloud computing," *CNET News.* Online resource, http://news.cnet.com/8301-13953_3-10052188-80.html, 2008.

[2] Mell, P., & Grance, T. "The NIST definition of cloud computing (Special Publication 800-145)," Online resource, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 2011.

[3] *Id.*

[4] Intel IT Center. "Peer research cloud security insights for it strategic planning," Online resource, http://www.intel.com/content/dam/www/public/us/en/documents/reports/cloud-computing-security-for-it-strategic-planning-report.pdf, 2011.

Cloud computing is one of the most significant delivery model paradigm shifts in the business use of technology. Industry analysts predict that spending on cloud computing will increase at an annual rate of 20% for years to come, growing to a global market of over $160 billion by 2013.[5]

LEGAL ISSUES IN CLOUD COMPUTING

Cloud users access the cloud by entering into a contract with a cloud service provider. In this section, we identify and analyze several key legal issues associated with cloud computing contracts. Next, we propose legal and practical strategies for dealing with them.

Most of the concerns that prospective cloud users have relate to the risk of disruption of service. This concern is well-founded because disruption of service can occur at any point in the complex infrastructure that provides the essential series of connections from the user to the cloud.[6]

Several categories of persistent concerns about cloud computing have been expressed by users and a representative list of these is set forth below.[7] Prospective cloud users frequently ask questions like these:

Access —Will I be able to access and use the cloud where and when I wish without hindrance from the cloud provider or third parties?

Reliability —Will the cloud provider be a dependable resource, operated by a reliable business entity?

Data Security —Will the cloud provider will prevent unauthorized access to both data and code, and will sensitive data will remain secure from electronic as well as physical threats such as floods, earthquakes, and fire.

Data confidentiality and privacy —Will the cloud provider, other third parties, and governments not monitor my activities, except when necessary for quality control purposes?

---

[5] Colarusso, D. "Note: Heads in the Cloud, A Coming Storm: The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection against Self-incrimination," *Boston University Journal of Science and Technology Law*. 2011.

[6] Kattan, I. R. "Cloudy privacy protections: Why the stored communications act fails to protect the privacy of communications stored in the cloud," *Vanderbilt Journal of Entertainment and Technology Law*, 13(617), 2011.

[7] Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing," *First Monday*, 14(5), 2009.

Liability —Is there a clear delineation of liability if serious problems occur?

Intellectual property —Will my intellectual property rights will be upheld and defended?

Ownership of data —Will I be able to regulate and to control the information that is created, modified, deleted or disseminated using cloud services?

Portability—Can data and resources stored in one area of the cloud be retrieved in a format that can be easily moved or transferred, if necessary, to another similar service with little or no effort? And, are there any unfair or unduly burdensome contractual obligations that hinder the process of moving the data?

Auditability —Will providers comply with regulations or at least be able to provide me with the necessary means to comply with any government requirements?[8]

Some of these concerns are closely related, such as security, confidentiality, and privacy. Others are discrete issues. For purposes of this paper, we focus our examination on the way in which typical contract terms in cloud service agreements address three related areas of concern: data security, privacy, and confidentiality. Some of the most prevalent forms of threats to these interests are identified, followed by a discussion of the various legal remedies available to injured parties when a dispute arises as a result of a failure to adequately protect data. The fear of a security breach is among the top concerns of cloud users and for that reason we have given special attention to legal issues that can be triggered by the tortious actions of third parties, commonly known as "hackers".

We offer the following brief definition of "hacking" for purposes of this discussion. A hacker has been defined as: "an individual who intends to gain unauthorized access to a computer system" using such means as spoofing, sniffing, Distributed Denial of Service attack (DDoS), identity theft, and other means.[9]

Hackers frequently seek to obtain personal information, such as social security numbers, driver's license numbers, or credit card numbers, in order to impersonate someone else. The information may be used to obtain credit, merchandise, or other services in the name of the victim or to provide the imposter with false credentials to be used for other nefarious purposes. The. According to the Identity Theft and Assumption Deterrence Act (ITADA) of 1998, identity theft is defined as follows: "Whoever knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or otherwise promote, carry on, or facilitate any unlawful activity that constitutes a violation of federal law."

Another federal statute (Title 18 United Stated Code § 1030) defines "computer crime" as "any violations of criminal law that involved a knowledge of computer technology for their perpetration, investigation, or prosecution. "

[8] Laudon, K., & Laudon, J. *Essentials of management information systems 9th edition*, 2011.
[9] *Id.*

According to a recent survey of IT professionals in the United States[10], the frequency, severity, and costs associated with hacking are rising. More than half of the organizations in the survey reported multiple breaches in the past year, and over forty percent experienced losses in excess of half a million dollars each. Further, the survey subjects reported that "[s]ecurity breaches most often occur at off-site locations but the origin is not often known. Mobile devices and outsourcing to third parties or business partners seem to be putting organizations at the most risk for a security breach."

Despite the coordinated efforts of law enforcement, hackers have been very busy lately. In the U.S. alone, there have been a total of 544,591,013 records breached in connection with the 2,931 known data breaches that have been made public since 2005.[11] According to a recent survey 81% of the responding organizations had experienced a security event during the past 12 months, compared to 60% in 2010. Presumably, there are many unreported breaches as well, so the actual number is higher.

Two hacker groups, known as "Anonymous" and "Lulzsec", claim responsibility for recent successful hacking episodes involving high-profile and presumably highly secure organizations: the Central Intelligence Agency, Sega, PBS.com, and the U.K. government.[12] These cases demonstrate the ability of hackers like Anonymous and Lulzsec to strike at will and on a grand scale.

State-sponsored cyber-attacks are increasing as well, and China[13] and Iran[14] have been identified as the leading suspects.

In a hacking attack against a company called Stratfor, nearly 900,000 email addresses and more than 68,000 credit card numbers were stolen from Stratfor and its clients, including powerful organizations such as Chevron, Sony, Lockheed Martin, Goldman Sachs, the United Nations, Google, AIG, HSBC, Bank of America, and the U.S. military.[15]

---

[10] Ponemon, L. "Cost of a Data Breach Climbs Higher," Online resource, http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher, 2011.

[11] Privacy Rights Clearinghouse. "Chronology of Data Breaches Security Breaches 2005 to Present," Online resource, www.privacyrights.org/data-breach, 2012.

[12] Oswald, E. "Hack Attacks Escalating? Here's a Reality Check," *Computer World*, Online resource, http://www.pcworld.com/article/230882/hack_attacks_escalating_heres_a_reality_check.html, 2011.

[13] Economist, "Masters of the cyber-universe: China's state-sponsored hackers are ubiquitous—and totally unabashed" Apr 6th 2013. From the print edition, and retrieved from online resource http://www.economist.com/news/special-report/21574636-chinas-state-sponsored-hackers-are-ubiquitousand-totally-unabashed-masters

[14] Nakashima, Ellen, "U.S. wary of warning Iran on cyber-attacks" The Washington Post 4-27-13, Online resource, http://www.washingtonpost.com/world/national-security/us-response-to-bank-cyberattacks-reflects-diplomatic-caution-vexes-bank-industry/2013/04/27/4a71efe2-aea2-11e2-98ef-d1072ed3cc27_story.html

[15] Sophos Ltd. "The State of Data Security Defending Against New Risks and Staying Compliant," Online resource, http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophosdatasecurityreportwpna.pdf, 2011.

An even more severe reported case involved as many as ten million credit card numbers compromised by unknown hackers in a data breach incident at a credit card processing company known as Global Payments, Inc.[16]

Still more embarrassing was an attack against Scotland Yard and the FBI which resulted in a Youtube posting of a discussion that took place during a conference call between the two intelligence agencies. The purpose of this call was to discuss how to best coordinate efforts to stop hackers.[17]

When a data breach occurs, the data owner and the company responsible for protecting the data face multiple issues in rapid succession. First, there are indirect costs such as lost sales revenues, notification costs, and the costs associated with breach detection and escalation of security counter-measures.[18] A recently released report on the cost of data breaches shows that costs continue to rise. In 2010, the costs of a data breach averaged $214 per compromised record and averaged $7.2 million per data breach event.[19]

The second costly consequence of a hack attack is the prospect of one or more lawsuits. For example, shortly after the Stratfor hacking episode, a class action lawsuit was filed against Stratfor in New York, alleging negligence, breach of contract and violation of the federal Stored Communications Act.[20] The plaintiffs demanded more than $50 million in damages on behalf of customers whose personally identifiable information[21] and credit card information was exposed. The case was later settled for an amount reported to exceed $2 million.[22]

In *Stevens v. Amazon.com* (2012),[23] a customer of online retailer Zappos filed a class action suit, on behalf of herself and 24 million other customers, against Amazon

---

[16] Kosner, A. W. “"Massive" Credit Card Breach of Estimated 10 Million Accounts: Where Are Those Smart Cards?” *Forbes*. Online resource, http://www.forbes.com/sites/anthonykosner/2012/03/31/massive-credit-card-breach-of-estimated-10-million-accounts-where-are-those-smart-cards, 2012.

[17] BBC News US & Canada. “Anonymous gain access to FBI and Scotland Yard hacking call,” *BBC News US & Canada*, Online resource, http://www.bbc.co.uk/news/world-us-canada-16875921, 2012.

[18] Ponemon Institute LLC, “Perceptions about Network Security,” Online resource, http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf, 2011.

[19] *Supra*, note 10.

[20] Ladendorf, K. “Austin-based Stratfor faces lawsuit over data breach,” *Statesman.com*, Online resource, http://www.statesman.com/business/technology/austin-based-stratfor-faces-lawsuit-over-data-breach-2139417.html, 2012.

[21] Wikipedia contributors. “Personally identifiable information,” Online resource, retrieved August 2, 2012, http://en.wikipedia.org/wiki/Personally_identifiable_information, 2012.

[22] Katz, B, “Stratfor to settle class action suit over hack,” *Reuters*, Online resource, http://in.reuters.com/article/2012/06/28/us-stratfor-hack-lawsuit-idINBRE85R03720120628, 2012.

[23] Stevens v. Amazon.com (Case No. 3:12cv-32 M), U. S. District Court for the Western District of Kentucky, Louisville Division Louisville, KY. Online resource, http://www.insideprivacy.com/ZapposCplt.pdf, 2012.

(the owner of Zappos), alleging loss of personal customer account information to unknown persons (hackers).

Heartland Payment Systems, an outsourced cloud payment processing service, was sued in U.S. District Court in Texas by nine banks over a data security breach that was announced in early 2009. The complaint alleged negligence, violation of consumer protection laws, and breach of contract. Not only did the banks sue, but so did the banks' customers. The claims were reportedly settled for a total cost of $4 million.[24]

In a case against an online cloud storage provider Dropbox Inc., plaintiffs alleged failure to secure users' private data or to notify the vast majority of them about a recent data breach.[25]

Win or lose, such litigation can be very costly, and many organizations may decide to reduce the number of the claims by offering to provide free credit monitoring services and/or pay for identity theft insurance for affected individuals. For example, the University of Hawaii settled a class action lawsuit filed on behalf of 96,000 people whose data was allegedly breached agreeing to "provide two years of credit monitoring and credit restoration services to those whose personal data was exposed online and who participated in the lawsuit."[26] [27]

Contracting in the Cloud

Cloud computing contracts typically take the form of a Subscription Agreement (the basic contract) together with a Service Level Agreement (SLA).The SLA contains an ancillary set of terms that are appended to the subscription agreement between a cloud service provider and a cloud service consumer. The SLA specifies, in measurable terms, the types of services and guarantees about delivery of those services that will be provided. According to the NIST, a survey of publicly available SLAs showed that while

[24] Vijayan, J. "Court dismisses most breach claims against Heartland by banks," *Computer World*, Online resource, http://www.computerworld.com/s/article/9222549/Court_dismisses_most_breach_claims_against_Heartland_by_banks, 2011.

[25] Hylkema, J. "Online storage provider Dropbox sued over data breach," *Thomson Reuters News & Insight*, Online resource, http://newsandinsight.thomsonreuters.com/California/News/Journal/2011/07_-_July/Online_storage_provider_Dropbox_sued_over_data_breach, 2011.

[26] Roman, J. "University Breach Lawsuit Settled - 96,000 Receiving Credit Monitoring, Restoration Services," Online resource, http://www.bankinfosecurity.com/university-breach-lawsuit-settled-a-4453, 2012.

[27] Schaffhauser, D. "U Hawaii Settles Data Breach Class Action Suit. Campus Technology," Online resource, http://campustechnology.com/articles/2012/01/30/u-hawaii-settles-data-breach-class-action-suit.aspx, 2012.

numerous cloud SLAs exist, there is little harmonization between the different types, key elements, and vocabulary.[28]

IT professionals have indicated in a recent survey that there is a lack of confidence in the contract terms offered by cloud providers. The survey results listed "Service level agreements (SLAs) [are] not bulletproof enough" as one of the top ten concerns, with 18% of respondents agreeing with this observation.[29]

In the next section, we examine some selected contract clauses related to the key areas of data security, privacy, and confidentiality from four of the leading cloud providers (Amazon Web Services, Microsoft Azure, Salesforce.com, and Google Apps for Business) and assess how effectively they address cloud users' top concerns.

Selected Cloud Computing Contract Clauses Related to Data Security, Privacy, and Confidentiality

In this section, we set forth selected contract clauses offered by cloud providers relating to the key problem areas of security, privacy, and confidentiality. We provide commentary on these examples and conclude with a description of strategies to mitigate risks to cloud users in those situations where the contract terms do not adequately address those risks.

Amazon Web Services (Security)

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

Comment: The language "we will help *you* secure *Your* Content" suggests that the burden of providing protection rests primarily if not completely on the user, not the provider. Further, "we will implement" falls short of "we guarantee" and "reasonable and appropriate" are not defined. Who decides what is reasonable or appropriate? We suggest that a recognized industry standard be incorporated by reference in this clause, for example: "we will implement security measures that are consistent with verifiable PCI compliance audits or with FedRamp certification standards."

[28] Badger, L., Bernstein, D., Bohn, R., Hogan, M., Leaf, D., Mao, J., Messina, J., Mills, K., Sokol, A., Tong, j., Vaulx, F., & Whiteside, F. "U.S. Government Cloud Computing Technology Roadmap Volume II: Useful Information for Cloud Adopters. (Special Publication 500-293 (Draft))," Online resource, http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf, 2011.

[29] Oswald, E. "Hack Attacks Escalating? Here's a Reality Check," *Computer World*, Online resource, http://www.pcworld.com/article/230882/hack_attacks_escalating_heres_a_reality_check.html, 2011.

Salesforce.com (Confidentiality)

8. CONFIDENTIALITY
8.1. Definition of Confidential Information. As used herein, "Confidential Information" means all confidential information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. ****

8.2. Protection of Confidential Information. The Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) (i) not to use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorized by the Disclosing Party in writing, to limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein.

Comment: This clause implies that the provider typically employs a standard of care that exceeds "reasonable" and that will be the standard provided to users. However, a lower standard (not less than reasonable) could also be in force in some situations which are undefined.

8.3. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

Comment: The open-ended exposure to costs, and reimbursement of costs, is a concern. There is no defined method for calculating "reasonable" costs, thus, should a dispute arise, a time-consuming battle about costs can be expected. Consider the following hypothetical case: A cloud provider is compelled by the U.S. Justice Department under authority of the USA Patriot Act to compile and provide copies of all of the emails generated by one of its users, a major bank, within a specified date range between parties X and Y. The bank, as the cloud client (Disclosing Party) would be forced to reimburse the cloud provider for these substantial unanticipated costs.

Microsoft (Privacy)

a) **Ownership of customer data.** As between the parties, you retain all right, title and interest in and to customer data. We acquire no rights in customer data, other than the rights you grant to us for the applicable online service. This does not apply to software or services we license you.

b) **Privacy.** Personal data collected through the online service may be transferred, stored and processed in the United States or any other country in which Microsoft or its service providers maintain facilities. This includes any personal data you collect using the service. By using this online service, you consent to transfer of personal data outside of your country. You also agree to obtain sufficient authorization from persons providing personal data to you, to:

- transfer that data to Microsoft and its agents, and
- permit its transfer, storage and processing.

See the online service's privacy statement for more information about how we may collect and use your information:

Privacy (Azure)
Microsoft regards personal information as private and will take reasonable and customary measures to appropriately handle personally identifiable information.

Microsoft (including, for this purpose, all of our U.S. subsidiaries) is Safe Harbor certified with the U.S. Department of Commerce. This allows for legal transfer of data to Microsoft for processing from within European Union and countries with aligned data protection laws. Microsoft acts as the data processor and, to the extent of the Service's capabilities, decisions regarding data usage are made by the data controller.

For information about specific data handling practices on the Windows Azure platform, please refer to the Windows Azure Platform Privacy Statement. The Windows Azure platform, like other Microsoft services and products, is built in accordance with Microsoft Trustworthy Computing Initiative's privacy guidelines.

Comment: The reference to data "transferred, processed, and stored" must be read in light of the very strict EU regulations on data protection. Data transferred into and stored in the EU may violate EU law when it is transferred out of EU jurisdiction, depending on what type of data is involved, where it is going, and perhaps who is controlling it. In this typical example of most cloud service provider contracts, responsibility for conforming to differences in location-based jurisdictional laws falls on the client to know and adhere to such legal differences. These jurisdictional differences are associated with the physical location of the provider's data centers. Since typical cloud service contracts imply that a client's data may be transferred at any time to another data center for *performance reasons*, the client may not even be aware of the transfer nor of the applicable laws now being enforced. Regional laws and designations should be identified, summarized, and maintained by each cloud provider, or a consortium of providers, and then made available to clients before the contract is negotiated and signed.

In addition, Microsoft does not permit outside audits by third parties, so in this clause it offers only to comply with its own internal guidelines as verified by its own internal employees.

Selected Contract Clauses Relating to Limitation of Liability

Liability for Loss or Destruction of Data

The typical contract language found in most cloud provider contracts offers little assurance to the user if data is lost or destroyed. In the next section, we set forth some cloud contract limitation of liability clauses, again followed by brief commentary.

Amazon (Limitation of Liability)

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

Comment: In this limitation of liability clause, Amazon clearly obligates itself to no more than the return of fees paid in the past year. In other words, no consequential damages (lost sales revenues) are permitted under these contracts. Note that the limitation includes "affiliates" and "licensors".

Microsoft

No Liability for Deletion of Customer Data. You agree that, other than as described in these terms, we have no obligation to continue to hold, export or return your customer data. You agree that we have no liability whatsoever for deletion of your customer data pursuant to these terms.

Limitation of Liability. Despite anything to the contrary in your volume licensing agreement, to the extent permitted by applicable law, our and our Affiliates' and contractors' liability arising under that agreement in connection with the Windows Enterprise Software is limited to direct damages up to the amount you were required to pay under the buy-out option.

Comment: Note Microsoft's direct approach to avoiding responsibility for customer data: "no obligation to hold, export, or return." In other words, the data portability costs are the responsibility of the client.

In the next section, strategies for addressing cloud computing contract issues are proposed, including legal, practical, and regulatory proposals.

Strategies for Cloud Users

Legal Strategies

As the foregoing discussion has indicated, cloud users have significant and persistent concerns relating to the risks inherent in cloud computing. Unfortunately, those concerns are not adequately addressed in the standard contract terms offered by most cloud computing vendors. The fact is that these contracts heavily favor cloud vendors and most cloud users lack sufficient bargaining power to negotiate more balanced agreements. Nevertheless, there are some legal strategies cloud users can implement to mitigate some, but not all, of these concerns.

Data Security

Data security is a major concern for most cloud users, however many cloud vendors will not guarantee anything but an agreement to provide "reasonable data security" in their contract terms.[30] Of course, "Reasonable data security" is language that favors vendors, so cloud users should attempt to negotiate a level of data security that can be incorporated into the contract by reference to a named specific compliance audit standard. Better yet would be to have that specified level of security verified based on an inspection and certification arrangement with an independent security organization and further require that the certification of compliance be updated regularly and communicated to both parties.[31]

Ownership of Data

Another legal concern for cloud users is the ownership rights in data. The cloud user's ownership rights in its data may appear to be exclusive and unquestioned, however cloud users should insist that the contract terms explicitly state that vendors hold absolutely no property rights to the user's data, and that the user retains all right, title, and interest in its data at all times and for all purposes.[32] Further, users should require terms that stipulate that their data must not be shared with subsidiaries or third party affiliates with express written consent of the client.

Data Confidentiality

In some cases, specific industries must use additional diligence to protect end user data. Cloud users should include specific terms that account for HIPAA, FERPA, and other data-specific confidentiality regulations.[33] This should be an explicit part of cloud

---

[30] McDonald, S. "Legal and Quasi-Legal Issues in Cloud Computing Contracts," Online resource, http://net.educause.edu/section_params/conf/CCW10/issues.pdf, 2012.

[31] Cloud Industry Forum, "USA Cloud Adoption & Trends 2012," Cloud Industry Forum. Online resource, http://www.cloudindustryforum.org, 2012.

[32] *Supra*, note 30.

[33] Hogan Lovells. "Cloud Computing: A Primer on Legal Issues, Including Privacy and Data Security Concerns," Online resource, http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/docs/Cloudprimer.pdf, 2011

contract terms, and should be updated regularly or whenever regulations change. Furthermore, all cloud users should include explicit sections that prohibit data mining of any kind without express permission of the data owner.

Liability

Cloud users always have concerns with liability for loss of information due to hacking, or system downtime. Although cloud vendors are solely in control of the security of data, they typically seek to release themselves from any liability for loss of data.[34] Cloud users should attempt to negotiate to remove limitations of liability and to insert terms holding vendors accountable for losses caused by the vendor's negligent actions.[35]

Practical Strategies

In addition to legal strategies, cloud users' concerns can also be managed through practical cloud strategies. These practical strategies can be used in tandem with legal strategies to increase the cloud user's level of security and bargaining power.

Redundant systems

Many events can cause a catastrophic failure in a cloud vendor's system. Acts of God, bankruptcy, or market forces can cause a cloud vendor to lose data or shut down operations. To avoid loss of business due to damage or lost data, users can retain multiple cloud vendors to store different kinds of data. Dividing user data among different providers can also allow greater levels of privacy and confidentiality. Cloud users can store sensitive data in different clouds so that the data is unidentifiable, then reassemble the data later when needed for use.

Alternatively, cloud users may consider contracting with multiple cloud vendors to store all of their data redundantly. Although it is a more costly approach, using redundant cloud systems can reduce the risk of data loss or damage.

By using redundant systems cloud users may be able to leverage their bargaining power by setting up competition between vendors, thereby attempting to secure better contract terms. Lastly, redundant systems may remove the risk of lost data and disruption of service, minimize damage caused by hackers and reduce the risk of litigation. This may in turn make indemnification clauses and exculpatory clauses less burdensome to cloud users.[36]

---

[34] *Supra*, note 30.

[35] Cloud Industry Forum, "USA Cloud Adoption & Trends 2012," Cloud Industry Forum. Online resource, http://www.cloudindustryforum.org, 2012.

[36] Abu-Libdeh, H., Princehouse, L., & Weatherspoon, H. "RACS: A Case for Cloud Storage Diversity," Online resource http://www.cs.cornell.edu/~hweather/publications/racs-socc2010.pdf. 2010.

Private and Hybrid clouds

Private and hybrid clouds can be another avenue for a cloud user to mitigate legal concerns of cloud computing. Private and hybrid clouds allow a much higher degree of customization for cloud users.[37] Customizing a private or hybrid cloud to the users' needs can help to avoid some of the legal concerns with privacy, confidentiality and security. Private and hybrid clouds allow data to be stored in their own individual clouds, away from other data, and the risks of that data, that may come with public clouds.[38] Private clouds also offer a more symbiotic relationship between cloud users and vendors.[39] This can add to the bargaining power of cloud users, further mitigating legal concerns.

Encryption

Cloud users can encrypt their data during transmission to the cloud, as well as "at rest" (during storage in the cloud). The cloud vendor may offer encryption services to cloud users but why use the cloud provider's service? A more secure approach may be user-initiated and controlled encryption. Encryption may lessen or completely eliminate some of the legal concerns mentioned above since any data that is released to unauthorized parties will not be readable or useable without the encryption key.

Insurance

Cloud users can mitigate risk by buying cyber attack insurance. Cyber insurance has been around since the dotcom boom and bust, and historically covered liability, property, cyber-extortion, and crisis management/public relations coverage.[40] Until recently, this form of risk mitigation remained suitable only for large cloud provider companies. But insurance has become a more feasible option for the cloud user and the cloud provider.[41] Both parties should consider using it, and should contractually negotiate who should bear the insurance cost burden. Insurance is another tool for cloud users when negotiating advantageous contract terms, or to simply mitigate the risks the cloud provider is unwilling to take. Cyber insurance, however, is very expensive and requires that the applicant submit to an independent compliance audit as a condition of the contract.

---

[37] Gerber, A., Ramakrishnan, K. K., Shenoy, P., Van Der Merwe, J. & Wood, T. "The Case for Enterprise Ready Virtual Private Clouds," Online resource, http://static.usenix.org/event/hotcloud09/tech/full_papers/wood.pdf, 2009.

[38] Foster, I., Llorente, I., Montero, R. & Sotomayor, B. "Virtual Infrastructure Management in Private and Hybrid Clouds," Online resource, http://www.computer.org/csdl/mags/ic/2009/05/mic2009050014.html, 2009.

[39] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, L., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. "A View of Cloud Computing," *Communications of the ACM*: *Practice*, 53(4), 2010, 50-58.

[40] *Id*.

[41] Navetta. D. "Cyber Insurance: An Efficient Way to Manage Security and Privacy Risk in the Cloud?" Online resource, http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/cyber-insurance-an-efficient-way-to-manage-security-and-privacy-risk-in-the-cloud, 2012.

Industry Trends and Proposed Regulations

Cloud computing has been in need of regulation and legislation since its inception. Industry pressures have been pushing for more regulation, and there are some signs among regulators and lawmakers that there is an increasing willingness to take action soon. The question is not if there will be government regulation, but when it will happen and what it will look like.

Federal Regulation

The Federal Trade Commission (FTC) has moved toward influencing regulation of data technology and cloud computing by submitting recommendations to congress for future legislation. The FTC primarily focuses on creating a baseline or "default" privacy principles for data. Furthermore, the FTC approach pushes for self-regulating codes enforced by the FTC and The Department of Commerce,[42] more uniform privacy standards, and more transparency so consumers can better track the privacy policies of companies. This could change cloud users relationships with cloud providers as more cloud providers are forced to include contract provisions that incorporate privacy protections established via regulated standards.[43]

In July of 2012, a new cybersecurity bill was introduced in the U.S. Senate.[44] The proposed law would create a National Cybersecurity Council populated by the major government security agencies and empowered to identify and protect critically important information systems from cybersecurity threats. This bill, if enacted, may directly or indirectly influence industry standards and practices.

State Legislation

Many companies are reluctant to report computer crimes because the crimes may involve employees, or the company fears that publicizing its vulnerability will hurt its reputation. However, according to the National Conference of State Legislatures every state except Alabama, Kentucky, New Mexico, and South Dakota have passed legislation requiring public disclosure of data security breaches.[45] California's data breach law, one of the first security breach notification laws, "…requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is

[42] Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change," Online resource, http://ftc.gov/os/2012/03/120326privacyreport.pdf, 2012.

[43] Tsukayama, H. "FTC releases final privacy report, says 'Do Not Track' mechanism may be available by end of year," *The Washington Post*. Online resource, http://www.washingtonpost.com/business/technology/ftc-releases-final-privacy-report-says-do-not-track-mechanism-may-be-available-by-end-of-year/2012/03/26/gIQAzi23bS_story.html, 2012.

[44] *Supra*, note 1.

[45] National Conference of State Legislatures. "State Security Breach Notification Laws," Online resource, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx, 2012.

believed to have been disclosed)."[46] These state laws have far reaching implications; first, the victims of hacking must be made aware of the crime, and facilitating collaboration on class action litigation against negligent organizations. Second, cloud providers may build data centers in states without strong data security breach disclosure laws, such as South Dakota.

Industry Trends

Industry insiders are also pushing to influence laws regarding cloud computing. Within the cloud computing industry a self-organizing body has emerged. Open Cloud Standards Incubator or (OCSI) was created in 2009 by many of the tech giants[47] that were first introducing cloud technology. This new services management standards body collaborated to define standards for cloud computing. OCSI has primarily pushed to create transparent and uniform security standards throughout cloud systems.[48] The OCSI also promoted standard auditing procedures, and regular audits of security. However there is some worry that cloud users are not fully participating in the creation of these standards, leaving the standards dominated by vendors.[49]

Several tech giants have also proposed their own cloud service contract guidelines like AWS (Amazon), CSA (Cloud Security Alliance), and CCAA (Microsoft's Cloud Computing Advancement Act). A summary of representative cloud computing contract guidelines and their associated sectors is provided in Table 1.

[Insert Table 1 Here]

[46] Official California Legislative Information. "California Codes Civil Code (Section 1798.29 and 1798.82)," Online resource, http://www.leginfo.ca.gov/calaw.html, 2012.

[47] Distributed Management Task Force. Inc. "Interoperable Clouds: A White Paper from the Open Cloud Standards Incubator," Online resource, http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf, 2009.

[48] *Id.*

[49] *Supra*, note 17.

It would be naïve to assume that cloud service providers, government and private sector clients, and professional industry associations will agree to develop a set of consistent contract guidelines. Therefore, it is more likely that the fairness of cloud computing contract terms will measured against the standards contained in the US Federal Government proposed FedRamp Certification. FedRamp Certification is an initiative that is intended to standardize security regulations that cloud service providers must meet in order to be eligible to win contracts with government agencies and to enforce consistency among governmental bodies.[50]

While the FedRamp Certification proposal may strike some as "just more expensive government regulations," this may not, in fact, be the case. The business and legal costs associated with developing and maintaining the current myriad of different contracts is quite high when compared to a more standardized, consistent approach. In short, variability costs money. Stakeholder comments should be invited and taken into consideration when modifying and maintaining the FedRamp Certification guidelines on an on-going basis. The FedRamp proposal is considered to be *guidelines*. Certainly, additional terms can be added to contracts to fit the particular needs of a client and the engagement situation. In recognition of this fact, the authors are not proposing a uniform boilerplate cloud service contract, *per se*. Instead, we suggest that "***principles-based***" (as defined by European accounting standards) guidelines and representative clauses should be made available and explained so that they are well understood by all parties.

Conclusions and Future Research

Cloud computing continues to grow in popularity despite the numerous risks that remain associated with it. The cost savings may seem to be attractive enough to outweigh the risks for many enterprises, but any savings realized could quickly evaporate with a single hacking incident, a cloud provider's unexpected interruption of service, or a sudden lack of accessibility to data due to a power outage or natural disaster. Furthermore, cloud providers and their data centers are attractive targets for hackers because of the sheer volume and diverse nature of information they maintain. They are also especially vulnerable to large stakes lawsuits brought by hundreds or thousands of cloud users potentially affected at the same time as a result of a single data breach incident.

Cloud computing contracts generally are structured to protect the interests of the provider, not the user, and users have little bargaining power to alter the terms. Nevertheless, some actions can be taken to mitigate the effects of the asymmetrical bargaining power of the parties. It is possible for industry sectors to form buying

[50] Parizo, E. B. "FedRAMP certification draws interest; cloud monitoring guidelines coming soon," *SearchCloudSecurity*, Online resource, http://searchcloudsecurity.techtarget.com/news/2240157002/FedRAMP-certification-draws-interest-cloud-monitoring-guidelines-coming-soon, 2012.

coalitions and thereby increase their bargaining power for concessions in contracts with cloud providers. It remains to be seen if a federal regulatory guidelines approach and/or industry buyer coalitions will evolve.

Many users see proposed federal and state legislation as a positive development that could ease their level of concern about cloud computing. Taking the most optimistic view, a more regulated cloud industry in the future would push cloud vendors to better address the concerns of users and provide greater fairness in the contract terms they offer.[51]

Future research should investigate other legal concerns associated with cloud computing contracts such as accessibility, data portability, and international intellectual property protection when outsourcing to cloud providers. This study was written largely from the perspective of the clients of cloud providers. Future research should also investigate the cloud provider's points of view. Further research can inform efforts to develop transparent, fair, and uniform contract guidelines which address the concerns of both cloud users and cloud vendors.

[51] *Supra*, note 35.