Issues in TECHNOLOGY Innovation

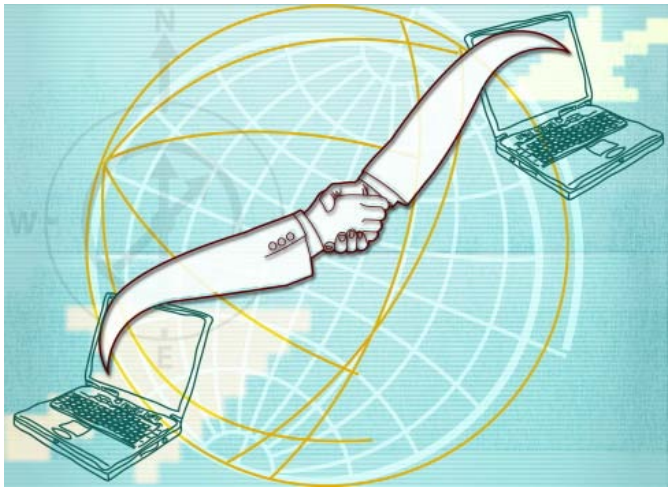
Number 7 March 2011

The Terms They Are A-Changin'... Watching Cloud Contracts Take Shape

Simon Bradshaw, Christopher Millard, and Ian Walden

EXECUTIVE SUMMARY

Many web services are examples of cloud computing, from storage and backup sites such as Flickr and Dropbox to online business productivity services such as Google Docs and Salesforce.com. Cloud computing offers a potentially attractive solution to customers keen to acquire computing infrastructure without large up-front investment, particularly in cases where their demand may be variable and unpredictable, as a means of achieving financial savings, productivity improvements and the wider flexibility that accompanies Internet-hosting of data and applications.



© Natalie Racioppa

The greater flexibility of a cloud computing service as compared with a traditional outsourcing contract may be offset by reduced certainty for the customer in terms of the location of data placed into the cloud and the legal foundations of any contract with the provider. There may be unforeseen costs and risks hidden in the terms and conditions of such services.

This document reports on a detailed survey and analysis of the terms and conditions offered by cloud computing providers.

The survey formed part of the Cloud Legal Project at the Centre for Commercial Law Studies (CCLS), within the School of Law at Queen Mary, University of London, UK. Funded by a donation from Microsoft, but academically independent, the project is examining a wide range of legal and regulatory issues arising from cloud

Issues in Technology Innovation

The Center for Technology Innovation at Brookings has launched its inaugural paper series to seek and analyze public policy developments in technology innovation.

The Center for Technology Innovation

Founded in 2010, the Center for Technology Innovation at Brookings is at the forefront of shaping public debate on technology innovation and developing data-driven scholarship to enhance understanding of technology's legal, economic, social, and governance ramifications.

Simon Bradshaw is a consultant for the Cloud Legal Project at the Centre for Commercial Law Studies (CCLS), Queen Mary, University of London. A former IT Engineer in the RAF, he qualified as a Barrister in 2009.

Christopher Millard is Professor of Privacy and Information Law at CCLS, where he is Project Leader for the Cloud Legal Project. He is also a Senior Research Fellow at the Oxford Internet Institute, University of Oxford, and is Of Counsel to Bristows.

Ian Walden is Professor of Information and Communications Law at CCLS and Consultant to Baker & McKenzie.

computing. The project's survey of 31 cloud computing contracts from 27 different providers, based on their standard terms of service as offered to customers in the E.U. and U.K., found that many include clauses that could have a significant impact, often negative, on the rights and interests of customers. The ease and convenience with which cloud computing arrangements can be set up may lull customers into overlooking the significant issues that can arise when key data and processes are entrusted to cloud service providers. The main lesson to be drawn from the Cloud Legal Project's survey is that customers should review the terms and conditions of a cloud service carefully before signing up to it.

The survey found that some contracts, for instance, have clauses disclaiming responsibility for keeping the user's data secure or intact. Others reserve the right to terminate accounts for apparent lack of use (potentially important if they are used for occasional backup or disaster recovery purposes), for violation of the provider's Acceptable Use Policy, or indeed for any or no reason at all. Furthermore, whilst some providers promise only to hand over customer data if served with a court order, others state that they will do so on much wider grounds, including it simply being in their own business interests to disclose the data. Cloud providers also often exclude liability for loss of data, or strictly limit the damages that can be claimed against them – damages that might otherwise be substantial if a failure brought down an e-commerce web site.

Although in some U.S. states, in E.U. countries and in various other jurisdictions the validity of such terms may be challenged under consumer protection laws, users of cloud services may face practical obstacles to bringing a claim for data loss or privacy breach against a provider that seems local online but is, in fact, based in another continent. Indeed, service providers usually claim that their contracts are subject to the laws of the place where they have their main place of business. In many cases this is a US state, with a stipulation that any dispute must be heard in the provider's local courts, regardless of the customer's location.

Perhaps the most disconcerting discovery of the Cloud Legal Project's survey was that many providers claimed to be able to amend their contracts unilaterally, simply by posting an updated version on the web. In effect, customers are put on notice to download lengthy and complex contracts, on a regular basis, and to compare them against their own copies of earlier versions to look for changes.

The cloud computing market is still developing rapidly, and potential cloud customers should be aware that there may be a mismatch between their expectations and the reality of cloud providers' service terms, and be alive to the possibility of unexpected changes to the terms.

Introduction

Imagine that a person hired a storage unit. Would they be perturbed to find a clause in the storage company's standard terms that disclaimed all liability for loss or damage to their property whilst in the storage company's custody, irrespective of cause? How would someone who hired a car for a week react if the rental company told them to check its website every day in case it had changed the permitted daily mileage? What would a business's views be of an accounting firm that would disclose the business's draft tax return to a third party if the firm felt it to be in its own best interests to do so?

It is safe to say that many businesses would have substantial reservations about entering into an agreement on such terms, whilst individuals – at least, legally savvy ones – might argue further that such clauses would be so unfair as to be unenforceable under consumer protection law. But every day consumers and corporations sign up to agreements for cloud computing services that contain terms corresponding to the examples above. At Queen Mary, University of London, U.K., the Centre for Commercial Law Studies' Cloud Legal Project has recently investigated such contracts. Our research shows that such terms are by no means uncommon. In this document we will examine in brief some of the issues our survey uncovered.

Cloud providers offering not specific servers but rather a flexible quota of processing and storage capacity... The great advantage of this, for both customer and provider, is that it becomes easy to accommodate variable demand.

What is Cloud Computing?

Cloud computing is clearly a topic of much interest currently. But what is cloud computing, and why is it different from conventional IT outsourcing? It can best be thought of as the provision of IT services as a utility, much in the manner of electricity. As Nicholas Carr has pointed out in *The Big Switch* (Carr, 2008), the early 20th Century saw industry move from private generating plants – with their own costs and demands for technical expertise – to grid supply from electricity providers. Today, we do not care where our electricity comes from, so long as it meets the required voltage and is available when we need it and in the quantity we require. IT services are moving the same way, with cloud providers offering not specific servers but rather a flexible quota of processing and storage capacity. The great advantage of this, for both customer and provider, is that it becomes easy to accommodate variable demand. From the customer's perspective, only as much capacity as is required at any time need be used and paid for. If, for example, the customer is running an e-commerce business with very seasonal sales (such as holiday bookings or tax return processing) then servers can be set up via the cloud as needed, and released when demand eases. This avoids the wasteful practice of provisioning for maximum demand that is inherent in buying dedicated IT hardware, or even in long-term outsourcing.

But the utility model is also beneficial to the provider. If enough customers have such variable demand, then, taken together, their aggregate requirement is likely to be far less than the sum of their individual peak needs. A cloud provider should see little idle capacity; as server capacity is released by one customer, it can be allocated

to another. Such efficiencies, augmented by the economies of scale achievable through building large data centers, can result in cost savings that can be passed on to customers as lower prices.

Cloud Computing Services Are Easy to Obtain

Ironically, the ease with which a cloud computing contract can be set up may itself lead to legal problems. A conventional IT outsourcing project will usually be managed as a significant project with a detailed contract that will be reviewed carefully by the customer, and will typically be subject to extensive negotiation. A cloud contract, on the other hand, is of its nature much easier to enter into, given that much of the attraction of cloud services is the speed and flexibility with which IT resources can be procured. Compared with conventional IT outsourcing, cloud provisioning is more akin to signing up to an email service or broadband connection. Many providers allow online sign-up via credit card, subject to their standard terms and conditions, for immediate use of a service. An organization may thus see cloud services as not only more cost-effective than conventional outsourcing, but as quicker and simpler to arrange. The inherent risk of this is that just because an agreement is seen as quick and relatively cheap to enter into it might also be seen as not being worth subjecting to proper legal scrutiny, especially if it is offered on standard terms rather than via a mutually-developed contract. However, a deal by which an enterprise transfers its data and processing to an outside body has just as many legal ramifications if carried out via cloud computing as if by more traditional methods. Indeed, it may have more; the flexibility and location-independence of cloud services introduce new business risks, such as the inadvertent transfer of data to other jurisdictions, or a much murkier relationship between the customer and the provider that actually hosts the customer's data.

We have already noted that many cloud providers make it quick and easy to sign up to their services. Such online sign-up is invariably subject to the provider's standard terms and conditions, whereby the customer agrees to a 'click-wrap' contract by confirming acceptance of such terms.

Some cloud contracts will, however, be specifically negotiated in a manner similar to traditional outsourcing transactions. This may, for example, be because of their value, perceived risk or public profile (such as the recent agreement between Google and the City of Los Angeles). For the purposes of this survey, however, we concentrated on a range of terms and conditions that are offered for immediate online sign-up.

The QMUL Cloud Legal Project's survey reviewed in depth 31 sets of terms and conditions from 27 different cloud providers, based on their standard terms of service as made available or supplied to customers. The survey was carried out in January 2010; all terms and conditions were revisited in July and August 2010 to verify the accuracy of specific terms quoted in our report and to assess the nature and extent of any amendments.

The difference in numbers arises because some large providers (e.g. Google and Microsoft) offer more than one cloud service. Furthermore, the survey involved more than 31 individual documents, as many cloud providers issue terms and conditions comprising a set of documents that may include Terms of Service (sometimes called a Customer Agreement), a Service Level Agreement (SLA), an Acceptable Use Policy (AUP) and a Privacy Policy.

Location of Data

The location of customer data is likely to be a key concern for some customers, who will be mindful about the restrictions, for example, applying to the export of certain types of data from the US, or the export of "personal data" from the EEA.

Furthermore, it is not clear that all aspects of a service that a customer will be interested in will necessarily be included in the contract. The location of customer data is likely to be a key concern for some customers, who will be mindful about the restrictions, for example, applying to the export of certain types of data from the U.S, or the export of "personal data" from the EEA.

Amazon Web Services offers the option of restricting data storage to one of certain regions including the E.U. (specifically Ireland), U.S. Standard and U.S. West (Northern California) — see http://aws.amazon.com/s3/faqs/#Where_is_my_data_stored. However, the terms and conditions for Amazon Web Services do not contain any term that specifically warrants that data will be kept in a particular location. A customer is asked to select a data region during the sign-up process, and this, we suggest, would form a representation that would be incorporated into the customer's contract with Amazon. Nonetheless, customers should carefully scrutinize the terms and conditions of a prospective cloud provider to ensure that features or issues important to them are actually addressed by the contract.

Disputes and Jurisdictional Issues

Moving on from the nature of the contract, if a dispute should arise under it the first obstacle a customer might face would be in bringing an action in court, as the contract may well specify a foreign legal system and jurisdiction. Of the 31 terms and conditions in the survey, 15 claim to be governed by the law of a U.S. state – usually California, although the laws of Massachusetts, Washington, Utah and Texas were also invoked. Such terms are usually accompanied by a provision stipulating that the courts of the relevant state will be the sole venue for bringing a claim against the provider. Of the other 16, eight either specified English law generally, or stated that it would apply for a U.K. or European customer. Customers could therefore well find themselves being expected to travel to a court in another state or even country to argue a claim under commercial law with which they may not be unfamiliar. Although such terms are, in the E.U. and some other countries, generally void against consumers, it is doubtful how much meaningful legal recourse a private customer has against a provider based in another continent.

Confidentiality, Integrity, Availability and Security

Assuming a customer could overcome jurisdictional issues, what might be the issues that could prompt a legal dispute over cloud services? A customer will be contracting for storage and/or processing of data, and will probably assume that the provider will have obligations of confidentiality, integrity and availability (sometimes termed the 'CIA Triad' of data security). Confidentiality refers to the expectation that the customer's data will not be disclosed to third parties, either through security deficiencies or deliberate release; integrity to the expectation that data will not be lost or corrupted; and availability to the expectation that storage and processing services will work when required. Breach of these obligations may cause damage to the customer, particularly as indirect or consequential loss arising from, for example, an e-commerce site experiencing prolonged downtime.

A customer seeking to sue a provider over such breaches would, however, have to deal with exclusion clauses and disclaimers in the terms and conditions. Our survey found that most of the providers we examined made extensive use of such terms. Indeed, in some cases it is difficult to see how the contract, if taken at face value, could allow a dissatisfied customer any redress at all.

Take confidentiality and integrity, for instance. Many providers explicitly place responsibility for these matters on the shoulders of the customer; for instance, Clause 7.2 of the terms & conditions for Amazon Web Services (Amazon, 2010) states that:

> *"...you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications."*

It might seem reasonable to ask the customer to secure data; after all, the customer is in a position to encrypt and decrypt it. However, this is only simple for storage. If the data is to be processed actively in any way, then it has to be decrypted. At present this remains a major security concern for those potential cloud customers with particularly 'sensitive' data, whether 'sensitive' in the specific data protection sense e.g. health data, or sensitive for commercial or other reasons. This is because if it is to be subject to active processing operations (as distinct from mere storage) in the cloud then even if it is encrypted in transit it will have to be decrypted for such additional processing. A number of cryptographic researchers are seeking to develop so-called homomorphic encryption systems that would allow encrypted data to be processed securely without decryption, but such schemes require so much additional computing power as to be currently of little practical use (Simonite, 2010). For the time being, therefore, consumers will have to rely on providers for the security of their data whilst it is being processed (beyond simple storage), but an exclusion

clause like the one quoted above could make it difficult to bring a claim against a provider for inadvertent or negligent leaking of customer data.

Furthermore, such leaks may not actually be inadvertent. A cloud provider may well receive a demand for disclosure of a customer's data, for instance if the customer is suspected of involvement in crime or a tort against a third party such as copyright infringement. Some providers will only do so if legally compelled to; see, for example, Clause 8.4 of the terms and conditions of Salesforce.com (Salesforce, 2010):

> *"The Receiving Party [Salesforce.com] may disclose Confidential Information of the Disclosing Party [the customer] 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."*

Many providers have a rather lower disclosure threshold, however. ADrive.com states in Clause q of its terms and conditions (ADrive, 2010) that:

> *"You authorize ADrive to disclose any information about You to law enforcement or other government officials as ADrive, in its sole discretion, believes necessary, prudent or appropriate, in connection with an investigation of fraud, intellectual property infringement, or other activity that is illegal or may expose ADrive to legal liability."*

The risk to a customer posed by such a term is that a provider might well consider that it is prudent or appropriate to avoid the prospect of legal action and its associated costs by simply agreeing to a particular disclosure request.

Returning to the disclaimer from Amazon Web Services quoted earlier, it is worth noting that it also covers destruction and loss of data, and furthermore places the responsibility for backing up the customer's data with the customer. Such terms should give pause for thought to those customers who intend to use the cloud for backup of on-site data; in effect, they are being told to back up their backups. This is not to say that cloud-based backup is unwise; indeed, given that cloud providers typically use highly-redundant architectures in their data centers to ensure that multiple copies of data are stored, the chances of accidental data loss through hardware failure are much lower in the cloud than they are for on-site storage (Kommalapati, 2010). Nonetheless, such terms as that quoted would seem to deny liability for data loss caused by, for instance, deletion of a customer account through an administrative error.

A customer might run into similar problems attempting to bring a claim over poor availability. It is true that many paid cloud services are offered with Service Level Agreements (SLAs) that on their face provide compensation for unscheduled service outages. However, careful reading of typical cloud SLAs reveals that they may be of limited comfort to customers. To begin with, the terms and conditions often include a very restrictive definition of what counts as an outage. ElasticHosts, for instance, appears to offer a very impressive 100 percent availability target, but on closer inspection this excludes downtime caused by, among other factors

(ElasticHosts, 2010):

> *"Acts or omissions of you or your users.*
>
> *Software running within your virtual servers.*
>
> *Scheduled maintenance which we have announced at least 24 hours in advance.*
>
> *Factors outside our control, including but not limited to any force majeure events; failures, acts or omissions of our upstream providers or failures of the internet.*
>
> *Actions of third parties, including but not limited to security compromises, denial of service attacks and viruses."*

Whilst many of these exclusions are perfectly reasonable – it would be perverse to hold the provider responsible for a failure caused by the customer – they nonetheless mean that a '100 percent uptime guarantee' will not, in fact, be an assurance of a truly uninterrupted service.

The majority of providers – including all the U.S.-based providers in our survey – firmly exclude liability for damage arising from the use of their cloud services.

Limitations on Remedies and Liability

Even when a cloud outage is directly attributable to a failing of the provider, the remedy under the SLA may not be everything the customer might wish for. Without exception we found in our survey that cloud SLAs do not offer refunds of charges but rather service credits against future use; such credits are usually subject to a cap such as one month's standard billing. The issue here is that a customer who has experienced a serious outage may not wish to continue with a cloud provider that has offered poor service. Credits against future billing will be of little or no benefit to customers that decide to switch providers following unsatisfactory service.

A further issue with remedies for service outage arises from another very common feature of cloud terms and conditions. The majority of providers – including all the U.S. based providers in our survey – firmly exclude liability for damage arising from the use of their cloud services. This is particularly so in the case of indirect and consequential damages. The significance of this for customers is that the indirect costs of a cloud service failure are likely to dominate the losses suffered by a customer. If the online sales portal for a business is not available for several hours on what would normally be a busy day then the value of lost sales may well dwarf any service credit under an SLA. Such disclaimers can be very wide-ranging, such as that asserted by CloudHosts in Clause 9.3 of their terms and conditions (CloudHosts, 2010):

> *"...in no case will the Company be liable to the Customer [or] any third party for or in respect of any indirect or consequential loss or damage (whether financial or otherwise) or for any loss of data, profit, revenue, contracts or business however caused (whether arising out of any negligence or breach of the Agreement or otherwise) even if the event was foreseeable by, or the possibility thereof is or has been brought to the attention of the Company."*

Providers also seek to limit their liability in cases where they cannot wholly exclude it. We found that very often providers seek to cap their liability to a customer in terms of the amount paid by that customer over a set period (typically one month). As seen in this excerpt from the Limitations of Liability clause of the terms and conditions of Decho for its Mozy service (Mozy, 2010), for 'free' services this functionally equates to a total disclaimer of liability:

> *"WITHOUT LIMITING THE FOREGOING, THE TOTAL AGGREGATE LIABILITY OF DECHO, AND ITS SUPPLIERS, RESELLERS, PARTNERS AND THEIR RESPECTIVE AFFILIATES ARISING FROM OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT, IF ANY, PAID BY YOU TO DECHO FOR THE SOFTWARE OR SERVICES. IF THE SOFTWARE AND SERVICES ARE PROVIDED WITHOUT CHARGE, THEN DECHO AND ITS SUPPLIERS SHALL HAVE NO LIABILITY TO YOU WHATSOEVER."*

A customer who has suffered damage and loss as a result of a problem with a cloud computing service thus faces several obstacles in bringing an action against the provider responsible. The provider may be in a different part of the world; the contract may operate under the laws of another jurisdiction; the contract may seek to exclude liability for the loss suffered, or may limit liability to what is, in effect, a nominal amount. Admittedly, consumer customers, for example, in Europe, may be able to argue that such terms are unfair within the meaning of local consumer protection legislation. Nonetheless they could still face the challenge of recovering damages from a cloud provider based in a different continent.

The Terms They Are A-changin'...

In view of the issues discussed above, a prospective cloud customer is likely to want to examine the contract for a cloud service carefully. But we found that this will in many cases be an ongoing duty, because of the approach that many cloud providers take to amending their terms and conditions. A large portion of the contracts we analyzed included terms providing that the provider could amend the contract simply by posting an updated version on its web site; if a customer continues to use the service, this is deemed acceptance of the new terms. Given that this policy in effect places customers on notice to review and check their terms and conditions – which are often long and complex documents – one might expect that providers would clearly flag up any changes that they did make. Surprisingly, this is often not the case. Few of the terms and conditions we examined clearly highlighted any changes from their previous version, and only about half of them even stated a revision date. As such, a customer may not only be asked to check if the relevant contract has changed, but may have no way of finding out if there have in fact been changes without undertaking a laborious line-by-line comparison of the current published terms and conditions with an archived version. It is unlikely that such an exercise will be undertaken on a regular basis, if at all, by a typical customer, whether

a public sector organization, a business or a consumer.

Conclusions

Should, then, prospective users of cloud computing be concerned by such contractual provisions? Although some of the terms and conditions we have described appear alarming, they should be seen in the perspective of the IT services industry as a whole. Many cloud providers are based in the United States, and so operate within a legal culture that tends to have a more laissez-faire approach to, for example, exclusion and limitation of liabilities, than is typically the case in Europe. As such, some of the terms noted are perhaps not, in their wider context, as Draconian as they may at first appear. Furthermore, many cloud providers have a background in hosting and Internet service provision, where an arms-length relationship with customers, reinforced by broad contractual disclaimers, is commonplace. Indeed, it is notable that cloud service providers that have a track record of engaging in long-term, trust-based relationships with customers, such as Salesforce.com, tend to have terms and conditions that are noticeably more accepting of liability for service provision than we generally saw.

Many cloud providers are based in the United States, and so operate within a legal culture that tends to have a more laissez-faire approach to, for example, exclusion and limitation of liabilities, than is typically the case in Europe.

The contractual issues we have noted should thus be seen not as factors mitigating against use of cloud computing, (although they should be borne in mind if contemplating the move of particularly sensitive or mission-critical data to the cloud) but rather as matters to be researched carefully when evaluating prospective cloud providers. The following is a short but by no means exhaustive checklist of points that could usefully be considered when looking at a cloud provider's terms and conditions:

- What legal system does the agreement claim to be governed by and are there any limits on where, how or when a legal claim can be brought against the provider?
- Does the provider assert the right to vary the contract unilaterally? If so, what, if any, mechanism is there to notify customers?
- Are there any undertakings or disclaimers regarding security of customer data?
- What, if any, notice will the provider give regarding deletion of customer data?
- On what grounds will the provider disclose customer data to a third party?
- What causes of service outage are covered by the SLA? What is the form and level of compensation?

- Does the provider exclude or limit liability for damage under the agreement, particularly consequential damages such as business losses?

In conclusion, cloud computing is an attractive option for many customers due to various technical and commercial factors and, in particular, flexibility and potential cost savings. These positive drivers should not, however, lead customers to lose sight of the need for appropriate diligence in scrutinizing the terms under which such services are offered. Cloud computing is an immature and rapidly-developing market, and many customers may find that there is a mismatch between their expectations (driven, perhaps, by the extensive 'hype' regarding cloud computing) and the reality of the service terms offered by providers. The flexibility and value for money of cloud services often comes at the cost of a more arms-length relationship between customer and provider than in traditional outsourcing contracts, and we have seen this reflected in many of the terms and conditions we have analyzed. As cloud computing services are developed further they may, like more traditional clouds, prove to be both highly varied in shape and subject to sudden changes – including in their terms and conditions.

The Center for Technology Innovation
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
http://www.brookings.edu/techinnovation

Editor
Christine Jacobs

Production & Layout
John S Seo

Tell us what you think of this *Issues in Technology Innovation*.

E-mail your comments to techinnovation@brookings.edu

For a more detailed review of our research and conclusions, see S Bradshaw, C Millard and I Walden, 'Contracts for Clouds: Comparison and Analysis of the terms and conditions of Cloud Computing Services' (1 Sep 2010), available via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

This document forms part of the Cloud Legal Project http://www.cloudlegal.ccls.qmul.ac.uk at the Centre for Commercial Law Studies, Queen Mary, University of London. The authors are grateful to Microsoft for providing generous financial support to make this project possible. The views expressed within this document, however, are ours alone. We would also like to thank Kuan Hon for suggesting the title of this article.

References

ADrive, "Privacy Policy", 27 September 2010. http://www.adrive.com/privacy

Amazon, "Amazon Web Services Customer Agreement", 27 September 2010. http://aws.amazon.com/agreement/

Carr, Nicholas, "The Big Switch: Rewiring the World, from Edison to Google", Norton, 2008.

CloudHosts, terms and conditions, 2010. http://www.cloudhosts.co.uk/terms.html

ElasticHosts, "ElasticHosts Service Level Agreement", 27 September 2010. http://www.elastichosts.com/cloud-hosting/terms-of-service

Kommalapati, Hanu "Windows Azure Platform for Enterprises", MSDN Magazine, February 2010. http://msdn.microsoft.com/en-us/magazine/ee309870.aspx

Mozy, terms of Service, 27 September 2010. http://mozy.com/terms

Simonite, Tom, "Computing with Secrets, but Keeping them Safe", Technology Review, 11 June 2010. http://www.technologyreview.com/computing/25537/page1/

Salesforce, "Master Subscription Agreement", 27 September 2010. http://www.salesforce.com/company/msa.jsp