EJLT European Journal of Law and Technology

Response to EU Commission Public Consultation on Cloud Computing

Karen Mc Cullagh [1] [2]

Background

This is a collaborative submission from a group of academics based in the UK with expertise in Information technology law and related areas. The preparation of the response has been funded by the Information Technology Think Tank, which is supported by the Arts & Humanities Research Council and led by the SCRIPT/AHRC Centre for Research and Intellectual Property and Technology, University of Edinburgh.

This response has been prepared by Karen Mc Cullagh, a lecturer in IT, Media & Public Law and a member of Media@UEA at the University of East Anglia. In addition, this response is submitted by the following individuals: Dr Abbe Brown, University of Edinburgh, Professor Joseph Cannataci, University of Central Lancashire, Dr Catherine Easton, Manchester Metropolitan University, Karen Mc Cullagh, University of East Anglia, Judith Rauhofer, University of Edinburgh, Kevin Rogers, University of Hertfordshire, Felipe Romero Moreno, Oxford Brookes University, Joseph Savirimuthu, University of Liverpool, Professor Burkhard Schafer, University of Edinburgh.

Clouds for users

Question 1

Do you feel that in the cloud services you are currently using or have been evaluating (or are providing), the rights and responsibilities of both user and provider are clear?

No

Question 2

Please comment

A key issue is that cloud service providers often advertise their services on their website on a 'take-it-or-leave-it' contractual basis. Cloud users are thereby encouraged to accept the provider's terms without question, since cloud providers typically present their contracts as standard and do not invite negotiation over terms. Small and Medium Size enterprise (SME) cloud users are unaware that they have the right to negotiate contractual terms, and in any event, lack the negotiating power to do so. As a result, cloud users often accept standard contracts that are heavily biased in favour of the cloud service provider. For example, the Customer Agreement for Amazon Web Services state:

'We and our licensors do not warrant that the service offerings will function as described, will be interrupted or error free, or free of harmful components, or that the data you store within the service offerings will be secure or not otherwise lost or damaged. We and our licensors shall not be responsible for any service interruptions, including, without limitation, power outages, system failures or other interruptions... ' [3]

Question 3

Are you aware of the applicable jurisdiction in different types of disputes that could arise during your provision or use (or potential future use) of specific cloud offerings?

Yes

Question 4

Is there an alternative approach to the determination of jurisdiction that may work better both for users and providers?

Yes

Question 5

If yes, please comment

The cross-border nature of cloud computing makes it difficult to identify which legal system is applicable. Also, the applicability of laws depends on the type of legal issue, since for each type of issue (e.g. contract, criminal law, data protection, torts etc.) the jurisdiction may differ. Potentially, up to four legal systems may need to be considered e.g. the legal system of the country where the cloud provider is located, where the cloud user is based, where the data is stored, and the location of the individual to whom the data relates.

Mc Cullagh [4] analysed the SLAs of five of the market leaders in cloud computing. She found that Google Apps SLA states that the parties will be bound by the laws of the State of California, whilst the terms of service of Amazon's SLA states that they will be bound by the laws of the State of Washington. In contrast, her analysis indicated that the SLAs of GoGrid and Microsoft Azure are silent regarding applicable laws. [5] Where the SLA is silent as to choice of law, Rome I Regulation stipulates that the law of the country with which the contract is most closely connected is applicable. [6] Accordingly, the place of performance of the obligation (and therefore the competent court) will generally be determined under the law of the country where the cloud service supplier has its central administration; yet this is difficult to determine when cloud computing involves transnational data transfers. The choice of laws may have serious repercussions for European based SMEs since they may not be able to afford the inconvenience and expense of enforcing their rights in another country or continent, namely the USA. [7]

Question 6

Please comment

In concurrence with Parrilli, [8] this response advocates classifying SMEs as consumers when they enter into SLAs with cloud service providers. If so, the SLA would be regulated by the law of the country where the SME consumer has their habitual residence,if the cloud provider addresses this country through a website/portal. This would reduce costs for a SME if they needed to litigate. Furthermore, the parties would still be free to agree that another law (e.g. of a USA state) will govern the contract, but consumer protection rules of the country of residence of the consumer would still apply. [9] Thus, classifying a SME as a consumer would be advantageous as it would reduce the cost and complexity of bringing legal proceedings against a cloud provider which breaches a service level agreement.

Question 7

Do you feel that the question of liability in cross border situations is clear for cloud users and cloud providers?

No

Question 8

Why?

As outlined above, the cross-border nature of cloud computing makes it difficult to identify which legal system is applicable. Also, the applicability of laws depends on the type of legal issue, since for each type of issue (e.g. contract, criminal law, data protection, torts etc.) the jurisdiction may differ.

For data protection issues, the general rule is that the laws of the country where the data controller (likely to be the cloud user) is based. For contractual disputes, Rome I is relevant. It states that, subject to exceptions, a court should apply the law chosen by the parties. If the contract is silent about choice of laws, then Rome I states that; 'a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence.' [10] Thus, it is likely to be the law of the country in which the cloud user is based.

Where torts are the issue e.g. libel, negligent advice, infringement of confidential information etc. the decision of which law to apply will be decided by referring to Rome II. Rome II states that, subject to exceptions, the applicable law is the law of the country in which the damage occurs, irrespective of where the events giving rise to the damage occurred, or where the indirect consequences of that event occur. However, where both

the alleged liable party and the party suffering damage habitually reside in the same country at the time the damage occurs, then the law of that country will apply.

Legislative Framework

Question 1

Do you think there are updates to the current EU Data Protection Directive that could further facilitate Cloud Computing while preserving the level of protection?

Yes

Question 2

If yes, please describe

At present data controllers and data processers seek to discharge their obligations under Directive 95/46/EC through a mixture of model contracts and binding corporate rules. Tracey & Bruening assert that this approach is cumbersome and expensive to administer. [11] Accordingly, there have been calls for existing laws to be supplemented by the adopting an 'accountability'-based data governance model. Indeed, Pearson & Charlesworth suggest that cloud computing providers should move away from terms and conditions of service towards 'accountability' contracts between the client and the initial service provider (SP), and between that SP and other cloud providers. [12] This approach advocates that cloud users actively take ownership of information management by requiring strong contractual assurances from companies providing cloud computing services that they are capable of meeting those obligations and of safeguarding personal data no matter where it is transferred or processed. The advantage of this contractual approach is that it allows an initial service provider to enforce its policies along the chain. As well as having organisational policies, accountability could be supported through 'sticky' electronic data policies. [13]

However, whilst the accountability approach is a useful supplement to Directive 95/46/EC it cannot supplant it, as risks that cannot be addressed contractually will remain. For example, data generally has to be unencrypted at the point of processing, creating a security risk and vulnerability exploitable by cybercriminals. Additionally, only large corporate users are likely to have the legal resources to replace generic SLAs with customised contracts, since adding requirements to the vendor chain will increase the cost of the service.

Question 3

Are you aware of specificities in member state data protection rules, or other legislation, that prevent you from using/providing cloud services within the EU?

Yes

Question 4

If yes, please detail

When data is stored in the cloud, a user runs the risk that data will be accessed not only by law enforcement agencies in its country, but also by law enforcement agencies in the cloud service provider's country. Of particular concern to some cloud users is the US Patriot Act since it allows US enforcement agencies to demand that the holders of information provide the information to them. Although enacted primarily for anti-terrorism purposes, its provisions allow use for ordinary criminal investigations. The Patriot Act allows US law enforcement agencies to obtain data belonging to a cloud customer residing in a server farm of a US cloud service provider. Accordingly, if the data is sensitive it may not be appropriate to use US cloud service provider.

Question 5

From your perspective, would it be useful if model Service Level Agreements or End User Agreements existed for cloud services so that certain basic terms and conditions could easily be incorporated into the contractual agreements.

Yes

Question 6

If no, why not?

Question 7

If yes, further thoughts about this might/should work

A flowchart/diagram should be developed and made available through the websites of both cloud service providers and Information/Data Protection Commissioners. This should prompt a potential cloud user to consider key issues in a particular order, and provide simple explanations of key terms and conditions in SLAs. A brief checklist is provided below which builds upon a checklist developed by the Cloud Computing Project at CCLS, QMU, [14] and it includes:

- What legal system governs the cloud computing agreement, and are there any limits on where, how or when a legal claim can be brought against the cloud service provider?
- Does the cloud service provider assert a right to vary the contract unilaterally? If so, what notification mechanism will be employed to notify cloud users?
- Does the Cloud service provider comply with Directive 95/46/EC; in particular Safe Harbour requirements, if it is based in the US? Do subcontractors also comply with such data protection requirements?
- Does the agreement contain undertakings or disclaimers regarding the security of cloud user data?
- What length of notice, if any, will the provider give regarding deletion of cloud user data?
- In what circumstances will the cloud provider disclose cloud user data to a third party?
- What causes of service outages are covered by the form and level of compensation?

Global solutions for global problems

Question 1

What are the most important Cloud Computing problems that have to be discussed global level? Please list and explain.

- Clouds users are wary of being locked into a particular vendor. Thus, cloud service providers should make the cloud inter-operative to facilitate data portability, so that it is easy for cloud users to exit one service provider and move their data to another.
- Development of industry codes of practice, e.g. through the Cloud Industry Forum.
- Development of standard or model contracts in addition to industry codes of practice. However, if a self-regulatory approach is adopted, this response contends that Industry codes of practice must be fully enforceable, with suitable remedies for non-compliance; otherwise compliance is a goal rather than a necessity.

Question 2

Which would be right fora/approaches to tackle them? Please expand. Industry codes of practice - Cloud Industry Forum

Data Protection - Article 29 Working Party

---

[1] See http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=cloudcomputing. This response has been approved by the Executive of BILETA (the British and Irish Law, Education and Technology Association http://www.bileta.ac.uk/default.aspx) and is therefore submitted on behalf of BILETA

[2] Karen Mc Cullagh, Lecturer in Public, Media & IT Law, UEA Law School, University of East Anglia. Email: k.mccullagh@uea.ac.uk She is also a member of the executive committee of BILETA (British & Irish Law, Education & Technology Association). Her key research interests are data protection, e-government and the regulation of new technologies. Karen's publications include: Ch6 - Cloud Computing in Electronic and Mobile Commerce Law, in Wild, C., Weinstein, C., MacEwan, N., & Geach, N. (2011) *Electronic and Mobile Commerce Law: An analysis of trade, finance, media and cybercrime in the digital age,* (University of Hertfordshire Press)

[3] Amazon Web Service Customer Agreement, *(July 7, 2010)*, Section 11.5 http://aws.amazon.com/agreement/

[4] Mc Cullagh, K. Ch 6 - Cloud Computing in Wild, C., Weinstein, C., MacEwan, N., & Geach, N. (2011) *Electronic and Mobile Commerce Law: An analysis of trade, finance, media and cybercrime in the digital age,* (University of Hertfordshire Press)

[5] Google Terms of Service www.google.com/apps/intl/en/terms/premier_terms.html 15.10 'Governing Law'. 'This Agreement is governed by California law, excluding that state's choice of law rules. For any dispute relating to this agreement, the parties consent to personal jurisdiction in, and the exclusive venue of, the courts in Santa Clara County, California.'

[6] Rome I Regulation, regulates choice of laws for contracts entered into after 17 December 2009. Regulation (EC) No 593/2008 of the European Parliament and the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (OJ L177, 4 July 2008, pp. 6-16).

[7] Wild, C. *et al* (2005) 'Council Regulation (EC) 44/2001 and Internet Consumer Contracts: Some Thoughts on Article 15 and the Futility of Applying "In the Box" Conflict of Law Rules to the "Out of Box" Borderless World.' *International Review of Law, Computers & Technology*, Vol. 19, Iss. 1

[8] Parrilli, D. (2009) 'The Determination of Jurisdiction in Grid and Cloud Service Level Agreements' GECON, vol. 5745 of Lecture Notes in Computer Science, page 128-39 (Springer).

[9] Directive 93/13/EC of 5 April 1993 on unfair terms in consumer contracts [OJ L95, 21.4.1993, pp. 29-34].

[10] Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0016:EN:PDF

[11] Treacy, B. & Bruening. P. (2009) 'Cloud computing -- data protection concerns unwrapped,' *Privacy and Data Protection*, Vol. 9, Iss. 3, p.3

[12] Pearson, S. & Charlesworth, A. (2009) "Accountability as a Way Forward for Privacy Protection in the Cloud," CloudCom '09 Proceedings of the 1st International Conference on Cloud Computing

[13] Creese, S., Hopkins, P., et al. (2009) 'Data Protection-Aware Design for Cloud Computing' www.hpl.hp.com/techreports/2009/HPL-2009-192.pdf, (CloudCom 2009 Proceedings, Beijing, Springer LNCS, December) 'Sticky' electronic privacy policies: personal information is associated with machine-readable policies, which are preferences or conditions about how that information should be treated (e.g., that it is only to be used for particular purposes, by certain people or that the user must be contacted before it is used) in such a way that this cannot be compromised. When information is processed, this is done in such a way as to adhere to these constraints. These policies are associated with data using cryptographic mechanisms. The user can be assured that the data processor has correct instructions for each individual data item as to where it may be transferred and processed (e.g. outside of the EEA/Safe Harbour etc).

[14] Bradshaw, S. & Millard, C. & Walden, I. (2011) The Terms They are a-changing'...Watching Cloud Contracts take shape, *Issues in technology Innovation*, No. 7, p.10