Infopreneurship Journal (IJ)

Available online at **www.infopreneurship.net**
Infopreneurship Journal (IJ),
2013, Vol.1, No.1

biblio.ir

Cloud Computing and Risk: A look at the EU and the application of the Data Protection Directive to cloud computing

Victoria Ostrzenski, MAS

Researcher, Records in the Cloud, School of Library, Archival and Information Studies, University of Brithish Columbia, Vancouver, Canada; **Contact**: victoria.ostrzenski@alumni.ubc.ca

Abstract

The use of cloud services for the management of records presents many challenges, both in terms of the particulars of data security as well the need to sustain and ensure the greater reliability, authenticity, and accuracy of records. To properly grapple with these concerns requires the development of more specifically applicable and effective binding legislation; an important first step is the examination and identification of the risks specific to cloud computing coupled with an evaluation of presently applicable legislation. Within the context of the European Union, this type of analysis centres on the Data Protection Directive (Directive 95/46/EC), and its related instruments. This article examines the present legal framework governing cloud computing in the EU today, and highlights how the various Articles of the Data Protection Directive can be linked to particular concerns about the cloud in order to better safeguard users and providers engaged in cloud computing.

Keywords: cloud computing, data protection, Data Protection Directive, EU, records, Records in the Cloud, Regulation.

Introduction

Though the adoption of cloud computing is not new, there has nevertheless recently been a major increase in the discussion surrounding cloud computing, bolstered, as is often the case, by a surge in supply through the introduction of service packages on offer from numerous large-scale providers. Similarly, only in recent years have legal professionals joined the conversation, beginning the process of identifying how to apply specific legal instruments to exert an appropriate measure of control in this area. In order to produce applicable and effective binding legislation to direct cloud computing, an important first step is the identification and examination of the relevant risks and challenges, proceeding in concert with an evaluation of any present legislation currently applicable to matters of cloud computing. This requires extending the analysis to the wider issue of data protection.

In the European Union (EU), the European Commission began pursuing the development of a strong cloud computing strategy in 2012, adopting an *Opinion on Cloud Computing* as set out by the Article 29 Data Protection Working Party as well as producing a *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe (Communication on Unleashing the Potential of Cloud Computing)*. For the EU, the discussion on cloud computing is closely tied to assurances that any endeavour upholds first and foremost the EU's call for data protection, in particular as outlined in *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).* [i]

Problem Statement

As regards the management of records, the ability to maintain and ensure the security and privacy of personal data is a critical part of upholding the integrity of the digital record, a quality never more at risk than in the realm of cloud computing, where the nature of the environment poses considerable threats. This article focuses on the analysis currently underway in Europe, as reflected through the aforementioned documents. In assessing the various risks related to cloud computing, it highlights how the various Articles of the *Data Protection Directive* can be associated with particular concerns about the cloud as means to safeguard users and providers engaged in cloud computing. It links the imperative for data protection to a wider assurance of reliable maintenance and security of records managed in the cloud, examines how *Directive 95/46/EC* and other instruments are being considered by the European Commission and associated Committees in their discussions on envisioning a well-guided cloud strategy, and provides information on a proposal that will potentially strengthen how the EU proceeds in addressing cloud computing.

Due to differences in how jurisdictions address this issue, the scope of the discussion will be limited to the EU's particular situation, and will focus on EU-wide legal instruments, without delving into how distinct nations apply EU law. There is a benefit in taking this wide lens view: the EU's application of law to a greater community of nations portrays the dialogue on cloud computing at a level that necessarily extends beyond different country borders, and this in turn shows how this issue may be addressed on a wider scale.

Records in the Cloud

Organizations create, share, store, and use records (Stuart and Bromage 2010, 220). These records must be reliable, authentic, and accurate. Where digital records are being managed, data privacy and security are imperatives for organizations concerned with proper records management. Indeed, assurances of reliability, authenticity, and accuracy are far more problematic in the digital world than in the paper context, in particular where cloud storage of records is being utilized (Stuart and Bromage 2010, 220). The use of cloud services for the storage of records poses challenges and raises many questions, including:

- *How can confidentiality of organizational records and data privacy be protected in the cloud?*
- *How can an organization's records accuracy, reliability, and authenticity (i.e. identity and integrity) be guaranteed and verifiable in the cloud?*
- *How can an organization's records and information security be enforced in the cloud?* (Duranti 2012, 2-3)

In order to respond to these questions, research on this matter began in 2012 in the Records in the Cloud Project (Duranti 2013). Part of the initial research has involved analysis and review of the various legal frameworks implicated in discussions and assessments of the cloud and the issues of risk, security, and trust. The following is an exploration of the European Union's own evaluation of cloud computing thus far, where discussion of cloud security is firmly rooted in, and consistently returns to, the issue of data protection, examined in the EU's Data Protection Directive. This is due to the fact that the use of cloud computing inevitably raises concerns over the protection and privacy of data - concerns resulting from the reality that both the data owner (user) and the cloud services provider does often not know exactly where the data is located, whether and how data has been replicated, or whether or not retention and disposal have proceeded securely (Stuart and Bromage 2010, 220). Responding to the questions about cloud security and the management of records in the cloud is therefore inherently tied to an examination of how data protection has been articulated in the various relevant legal frameworks.

Cloud Computing: Overview

Cloud computing is defined by the European Commission (2012, 1) as "the storing, processing, and use of data on remotely located computers accessed over the internet". Summarizing Svantesson and Clarke, Norizwadi Ismail (2011, 251) identifies five points that define the nature of cloud computing and cloud computing as service. They are: (1) delivery of the service via a telecommunications network; (2) reliance by users on the service to access and/or process data; (3) holding of data by means of the user having legal control; (4) virtualization of resources in the course of use of the service, where virtualization results in a user not having a need to know what server of what host is delivering the service; and (5) use of the service subject to an agreement articulated by a contractual agreement. Further, Ismail reduces the picture of cloud computing to an activity defined by the actions of four key entities: the user, the service provider, the data, and the Internet (Ismail 2011, 251). Accordingly, the qualities of cloud computing that make it a quick and easy endeavour to engage in also perpetuate its underlying risks of rapid scalability, remote data storage, and use of shared services, which all contribute to the data protection and privacy issues found therein (Pearson and Charlesworth 2009, 133). A proper response requires aligning particular risks and their causes to the particular points of a legal instrument that addresses them.

Identifying risks in cloud computing:

Data Protection, the Data Protection Directive, and the work of the Article 29 Working Party

For the EU, the determination of what requirements cloud computing must uphold corresponds first and foremost to the tenets set out in the Data Protection Directive. To ground this discussion of cloud computing and data protection, it is useful to first present how the Data Protection Directive determines the scope of what "personal data" means, and then recount how a key body (the Article 29 Working Party) has stood the Directive against the particular conditions of cloud computing, where the protection of personal data can be at stake. To begin: the Article 29 Working Party (2012, 6), acting within the confines of the EU's legal and regulatory environment and in concert with the European Commission, has confirmed that the Data Protection Directive applies to all instances where personal data is processed via cloud computing services. The spirit of the Directive extends and applies to clients, cloud service providers, communications providers, as well as infrastructure providers and others (European Commission 2012a, 8).

The Data Protection Directive defines a number of key terms, a few of which are included here for ease of reference in the analysis that follows:

- ***Personal data****: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an*

identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

- ***Processing of personal data*** *('processing'): any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;*

- ***Controller****: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and mans of the processing of personal data.* (Directive 95/46/EC, 1995, art. 2)

Established by Article 29 of the Data Protection Directive, the Working Party on the Protection of Individuals (hereafter the Working Party), is responsible for examining relevant application of the Directive's measures as well as making recommendations on matters regarding the protection of persons in relation to the processing of personal data (Directive 95/46/EC, 1995, art. 30).[ii] As of July 1st, 2012, the Article 29 Working Party has produced and adopted an Opinion documenting how cloud computing raises issues related to data protection, providing instruction on how these risks can be reduced by adherence to particular points of the Data Protection Directive.

A key tenet of the Data Protection Directive is that in order for users' personal data to be protected, the users must be informed about who processes their data as well as for what purposes their personal data is processed. Article 6 of the Data Protection Directive states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes" (Directive 95/46/EC, 1995, art. 6). Article 7 further states that data is to be processed only where the subjects have unambiguously given consent, or other requirements have been met (Directive 95/46/EC, 1995, art. 7). In light of the conditions that typify cloud computing (summarized in the introduction), the Working Party (2012, 5) has identified two main categories of risk inherent to cloud services: the first has to do with a lack of control over the data in the cloud, while the second regards the lack of transparency related to the processing of data via cloud computing.

Concerning the former, it is clear that use of a cloud service implies that users move information, including personal data, into a system that is structured as a virtualized service. This means that, upon transfer of materials to the cloud, users no longer have full access to the sort of technical or organizational measures that would allow them to maintain complete control of the data (for later referral to it, this risk is called risk 1) (Article 29 Data Protection Working Party 2012, 5). The Working Party (2012, 6) identifies the following features of the cloud as causes that perpetuate this risk: (1) use of proprietary technology due

to vendor lock-in, which will complicate the transfer of data between different systems as well as the exchange of data between entities using different cloud services; (2) sharing of resources, as a cloud is a shared system on infrastructure shared among clients; (3) minimized availability of confidentiality, where law enforcement could potentially request disclosure of information directly to a cloud provider-- if acting outside the EU this could result in a breach of EU data protection law; (4) outsourcing by providers, where services may end up being facilitated by various providers without the client fully knowing who is looking after their contract; (5) limited availability of direct controls, due to a provider not allowing a user full reign over management tools; and (6) possible data leakage, where the provider has multiple clients, and persons acting on its behalf (in an administrator role) are equipped with enough privileged access to adversely affect the security of individual clients. Unaddressed, each and every one of these issues pose adverse risks as well as show a lack of adherence to the Data Protection Directive.

Concerning the second risk, clearly insufficient transparency results from an improper or incomplete outline of the full breakdown of a cloud provider's services, leading to a limited awareness of the actual situation a user may be engaged in with a provider (risk 2). The Working Party (2012, 6) has indicated that the following factors affect matters of transparency: an incomplete understanding of the chain of processing and whether multiple subcontractors may be involved; lack of knowledge as to where data may actually be geographically located upon processing and throughout the duration of storage in the cloud; and unknown transfer of data to countries outside the European Economic Area (EEA).

Applications of the Data Protection Directive to cloud services

The risks associated with cloud computing, due to the conditions outlined above, are to be addressed first and foremost through application of policies that follow the Commission's requirements for data protection, as outlined through the points attributed to various Articles of the Data Protection Directive.

Responding to risk 1 requires ensuring the data subject has an appropriate level of control over data; this assurance is supported by the confirmation of multiple conditions, as defined in subsequent Articles. Article 12 of the Directive states that a data subject must be able to acquire information about any data being processed, and receive such information in a reasonable fashion without undue delay or expense, as well as be able to rectify, block, or remove any data that may have been processed in a way not supported by the Directive (here resulting from incorrect or incomplete data) (Directive 95/46/EC, 1995, art. 12). The Working Party (2012, 8) has also identified that a clear and complete allocation of responsibilities between involved parties be explicitly articulated in order to avoid any oversights due to hidden players being involved in data transfer or storage. In a 2010 *Opinion on the concepts of "controller" and "processor",* the Working Party (2010, 26) points to Article 17, which establishes the requirement that a binding legal act be put into place to regulate the data controller (in cloud computing, this refers to the user of the cloud

services), and the data processer (i.e., the cloud provider). The Working Party (2010, 27) goes on to clarify that the Data Protection Directive permits multiple entities to hold the title of data processor in a given contract, so all should be named in any agreements and all are to abide by the agreement tied to the data controller. The Working Party (2012, 8) tasks the user of any cloud services, as a client, with ensuring that during any contractual process where small-scale providers and large-scale providers are involved, no agreement proceeds that includes clauses or terms of contracts unfairly preferential to the large-scale provider.

In response to risk 2 and the task of ensuring provisions are in place to provide for assurances of transparency, again the Data Protection Directive is at present the key relevant Directive for reference. Diminished transparency due to unknown outsourcing of cloud services by one provider to another EU-based provider is addressed in Article 7, which requires the data subject be in a position to give unambiguous consent for data processing (Directive 95/46/EC, 1995, art. 7). Article 10 requires that the data subject be provided with the identity of his controller(s) as well as information about any other recipients of the data (Directive 95/46/EC, 1995, art. 10). As a general requirement, Article 4 sets out that Member States involved in data processing ensure all activity proceed in line with the applicable national law (Directive 95/46/EC, 1995, art. 4). In a similar vein, diminished transparency resulting from transfer of data outside the EEA, also known as transfer to "third countries", is addressed by the Directive through measures set out by Article 25, which explicitly establishes that transfer of data is only permitted where the third country has ensured an adequate level of protection for personal data, as determined through an evaluation that is to include considerations for the nature of the data, proposed processing operations, country of origin and country of final destination, as well as the rules of law and security measures enforced by the third country (Directive 95/46/EC, 1995, art. 25).

According to Ismail (2011, 254), data protection is better safeguarded where obligations are fully and clearly articulated between all parties involved. In general, transparency concerns can be mitigated through the following practical measures: soliciting consent from the data subject; producing a contract that affirms knowledge of any sharing of functions between service providers for a data subject; use of other formal legal instruments that expressly obligate and include all concerned parties, including explicit identification of processors in the terms of use; as well as the identification of any secondary software that may be used in the delivery of cloud services and which may affect data security (Ismail 2011, 254; Article 29 Data Protection Working Party 2012, 11).

Responding to Data Protection Concerns: the Commission's recommendations

In the Commission's *Communication on Unleashing the Potential of Cloud Computing*, as with the Working Party's *Opinion on Cloud Computing,* the concern over data protection has been identified as a central concern for both users and providers (European Commission 2012a, 5). Further underscoring feelings of uncertainty is the fact that, by their nature, cloud computing processes can extend beyond jurisdictions, leading to ambiguity over applicable law beyond adherence to the EU-wide Data Protection Directive. In order to understand this, consider that in the EU, where a Directive is in place to address some matter, its presence and the instructions contained therein bind all Member States to adopt laws that carry all the terms contained within the Directive (Fordham International Law Journal 2011, 25). This means that, for all EU Directives passed, there are distinct national laws adopted by individual Member States. For practices like cloud computing, where activities and processes can implicate multiple Member States and their respective laws, the challenge is to identify what additional statutes to follow.

Such issues grow with the progress of technology that can extend across jurisdictions; as a response, the EU has proposed new legal frameworks to strengthen adherence to the points of the Directive at the level of the entire EU. In response to data protection concerns, the *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, presented at the beginning of 2012, appears to be a critical instrument for discussions on cloud computing, because it binds Member States to properly engage in responsible practice as well as adhere to the same principles, and, if implemented (pending for 2013), will ensure that "a single set of rules would apply directly and uniformly across all 27 Member States" (European Commission 2012a, 8). Proposed as two documents in the form of a Regulation and a Directive, the portion passed as a Regulation would be an instrument holding the same binding power as would a federal or United States national law in each country, requiring adherence (Fordham International Law Journal 2011, 25).

Accompanied by a likeminded Directive to support the trust of the Regulation, the proposal underscores how, due to scale, matters of data protection should be approached using enforceable legislation at the EU level, as such actions will be more effective than those taken by individual Member States (European Commission 2012b, 5-6). The Commission's Communication supports adoption of this proposed regulation as a key legal framework that would allocate means for the adoption of codes of conduct and standards for the cloud across the board in the EU, thereby increasing consumer trust (on the part of the user) as well as reduce administrative burden and compliance costs (on the part of the provider) (European Commission 2012a, 8).

Concluding Remarks

The European Union has begun expressly concerning itself with cloud computing, in particular tying its discussion to data protection and the related issues and threats that result from the conditions inherent to the utilization of cloud computing. As a first step to understanding how the EU's legal environment addresses cloud computing, this article has presented a review of the work set out in the Commission's *Communication on Unleashing the Potential of Cloud Computing* alongside the *Opinions* produced by the Article 29 Working Party, showing how present instruments identify the risks and challenges of cloud computing and point to the Data Protection Directive for guidance on the matter. It is clear that, for an issue as amorphous as "the cloud", this firm rooting in the Data Protection Directive will have to be supported by further EU-wide legal instruments. As for the management of records in the cloud, the ability to ensure the integral qualities of reliability, authenticity, and accuracy will only become concrete where a comprehensive cloud strategy has been developed.

References

Article 29 Data Protection Working Party. 2010. Opinion 1/2010 on the concepts of "controller" and "processor," WP 169.

_____. 2012. Opinion 05/2012 on Cloud Computing, WP 196.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995, O.J. L 281/31.

Duranti, L. 2012. "Records in the Cloud: Towards Interpares Trust." Paper presented at Fondazione Rinascimento Digitale, Florence, Italy, December. Accessed March 18, 2013. http://www.rinascimento-digitale.it/conference2012/paper_ic_2012/duranti_paper.pdf.

_____. 2013. "Records in the Cloud." Accessed March 18, 2013. http://www.recordsinthecloud.org.

European Commission. 2012a. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe, O.J. C _ (/* COM/2012/0529 final */).

_____. 2012b. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the

purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM 2012/10.

Fordham International Law Journal. 2011. "A Citation Manual for European Union Materials 2010-2011 Edition." *Fordham International Law Journal* 34: 25-27. Accessed March 18, 2013. http://filj.lawreviewnetwork.com/files/2011/10/EU_Citation_Manual_2010-2011_for_Website.pdf.

Ismail, N. 2011. "Cursing the Cloud (or) Controlling the Cloud?" *Computer Law and Security Review* 27, no. 3: 250-57.

Pearson, S., and Charlesworth, A. 2009. "Accountability as a Way Forward for Privacy Protection in the Cloud." *Lecture Notes in Computer Science* 59: 131-44.

Stuart, K., and Bromage, D. 2010. "Current State of Play: Records Management and the Cloud." *Records Management Journal* 20, no. 2: 217-25.

[i] In this article I refer to *Directive 95/46/EC* both as "*the Data Protection Directive*" and "*the Directive*".

[ii] The Working Party is composed of a representative from each Member State's data supervisory authority, a Commission representative, as well as a representative of the authority(/ies) established for Community institutions and bodies (Directive 95/46/EC, 1995, art. 29).