Cross-border flow of personal data in the Cloud: A European Perspective

University of Oslo

Faculty of Law

Candidate number: 8007

Supervisor: Olga Mironenko Enerstvedt

Submission deadline: December 1, 2011

Word count: 18000 (Max. 18000)

27.11.2011

Abstract

We are witnessing a seismic information technology growth continuing to create novel business models and business opportunities. One such enticing technology area is cloud computing. Businesses and professionals looking for better efficiency and minimal cost are paid-off with the advent of the cloud. It has done so by setting free the resources previously capped in 'keeping the lights on' for some innovation and research and reducing the cost of procuring IT infrastructure. The Internet, at same time in point, has enormously facilitated the flow of information across jurisdictions in unprecedented scale and speed than before. Despite this, the law couldn't keep in pace with the technological growth.

The use of cloud service requires the relocation of data in to servers of the cloud provider. With the surge for such activity emerges significant uncertainties *interalia*, on the legal bases to subscribe to cloud services, when adherence to cross-border data regulation is needed, issue of applicable law and jurisdiction and importantly security breaches as a result of access by third parties after the data have been placed in to the providers' server. It is within the thrust of this thesis to characterize these concerns.

Acronyms

APEC- Asia Pacific Economic Cooperation

A29WP- Article 29 Working Party

BCRs- Binding Corporate Rules

DPA(s)- Data Protection Authority(s)

ECD- E-commerce Directive

ECHR- European Charter of Human Rights

ECJ- European Court of Justice

EUDPD- European Union Data Protection Directive

IaaS- Infrastructure as a Service

OECD- Organization for Economic Cooperation and Development

PaaS- Platform as a Service

SaaS- Software as a Service

SWIFT- Society for Worldwide Interbank Financial Telecommunication

TRIPS- Trade-related aspects of Intellectual Property rights

Table of Contents

1 Chapter One: Introduction

1.1 Background

In the pre-cloud era, operating systems, applications and data were typically stored on an individual user's computer.[1] With the surfacing of cloud computing and the Internet, users can now store and access their data from remote servers from anywhere in the world. Arguably this is a paradigm shift in how computer resources are acquired.[2]

There are claims that the underlying concept of cloud computing dates back to 1961 when John McCarthy predicted that "computer time-sharing may lead to the provisioning of computing resources and applications as a utility".[3] In the 1990's the concept of grid computing has emerged with the idea of making computer power accessible the same manner as electric power grid.[4] Such concept has contributed to the uptake of the cloud as we know it today. The Internet was also believed to be the primary factor for cloud concept to become a reality.

Despite being hailed for the significant business benefits it has brought, cloud computing is fraught with certain concerns. Privacy, *interalia*, is one such concern. Privacy is a broad concept.[5] This paper focuses on the European Union Data Protection Directive (hereinafter EUDPD)[6] that protects one aspect of privacy (information control).[7] Most particularly, this paper will provide an appraisal of how cloud computing fits with the regime under EUDPD regulating transfer of personal data to

---

[1] Joint (2009) p.270

[2] Marchini (2010) p.1

[3] Jefery (2010) p.5

[4] Wallis (2008) p.[1]

[5] Hon (2011a) p.3

[6] Data Protection Directive 95/46/EC

[7] See accompanying text (n 36)

third country. The discussion is also relevant to non-EU entities as a result of the extra-territorial reach of these provisions and the Directive in general. Further the EUDPD, which is applicable in the European Economic Area (EEA), is claimed to be the most comprehensive regional instrument on the area. [8]

1.2 Legal Questions and Problems Considered

Cloud computing a highly complex information technology service is interwoven with many legal questions. The aim of this thesis is to cover some of the most important questions related with cross-border flow of personal data in light of the EUDPD. The main research questions identified are:

- When does cloud computing involve transfer of personal data to third country pursuant to chapter IV of EUDPD and what possible legal bases can be relied to use cloud service that involve transfer of personal data to third country?
- Which courts or judicial authorities have jurisdiction over matters involving cross-border cloud services?
- When does EUDPD apply to cross-border clouds?
- What are the security concerns in using cross-border cloud services and how they can be dealt with?

Also included are: how the data controller-processor distinction stands and what constitutes personal data, and what privacy challenges are emerging, in the cloud.

1.3 Research Method

The primary focus of this thesis will be on the privacy concerns in cross-border clouds. To substantiate such concerns I will apply traditional legal dogmatics. Therefore, I will consider the application of the provisions on cross-border flow of personal data under the EUDPD to the cloud. Cases, articles and legal perspectives will be largely drawn from EU level though examples will be given from member states and other jurisdictions when relevant. Scientific method will also be employed to depict the technology at hand when necessary.

---

[8] Bygrave (2002) p.30

1.4 Structure of the Thesis

The thesis has four chapters including this introductory part. The second chapter will elaborate the general concept of cloud computing, types and benefits of it**.**

The third chapter will give a thumbnail sketch of privacy in the cloud. In doing so, it portrays what constitutes personal data in the cloud and whether cloud providers fall under the controller or processor distinction. It also highlights some of the problems associated with current cloud services. An analysis of some cloud providers' privacy policies will also be provided.

The fourth chapter is tailored to address the question as to when does cloud computing trigger the cross-border data flow provisions, and what legal bases are available for using cross-border cloud services. Consent, commonly invoked legal ground, forms another discussion point. Also included in the chapter is discussion on applicable law and jurisdiction in the case of cross-border clouds, along with security concerns. The chapter ends with analysis of the judgment by European Court of Justice's (ECJ) on related matter. I will then conclude with my observations.

2 Chapter Two: Cloud Computing

2.1 Cloud Computing Defined

In common vernacular, a 'cloud' relates to the weather. Nevertheless the term cloud computing has become a metaphor for the Internet in recent years despite uncertainty as to what it actually means. Recent studies show that 41% of senior IT professionals don't know what cloud computing is and two-thirds of senior finance professionals are confused by the concept of cloud computing.[9] Though many definitions have been promoted, some of them are too wide to equate cloud computing with general Internet use while others are too narrow to uncover the real nature of cloud computing.

That in mind, cloud computing is: *"*the delivery of a computing capability (whether of an application software, an infrastructure or otherwise) by a provider remotely over a communications link allowing for no actual installation of the software or infrastructure at the customer site."[10]

However, this definition misses some of the key attributes that attracts customers to the cloud. Such features are *scalability* (the variability of the amount of computing capacity as per customer's requirements); *elasticity (*rapid response to changes in computing demand).[11]

Thus, cloud computing can be referred as the provision of resources (e.g. networks, servers, storage, applications, and services) which can be reconfigured easily to meet changes in demand from remote severs through some kind of network. Cloud computing is, however, an "evolving paradigm, meaning: its definition, attributes, and

[9] Jadhwanl (2009) p.1

[10] Marchini (2010) p.1

[11] Bradshaw (2010) p.4

characteristics are still being debated by the public and private sectors, and are certain to continue to evolve in the near future".[12]

The cloud provider, the user and the data subject are mainly the possible actors involved in cloud computing. The user is a customer or potential customer of a cloud service while a cloud provider is the organization that offers the cloud service. The data subject is the person him whose data is located in the cloud by the user.

2.2 Cloud Service Models

2.2.1 Software as a Service (SaaS)

SaaS is the capability provided to customers to use the provider's applications running on a cloud infrastructure.[13] The software is subscribed to, not licensed.[14] Simple illustration of the concept: - when Microsoft Office Word is not installed in your computer, SaaS allows you to create a word document by accessing the software from third party provider. The underlying resources (network, servers, operating systems, storage) are mainly controlled and managed by the provider.[15] For example, webmail services (e.g. G-mail).[16]

2.2.2 Infrastructure as a Service (IaaS)

IaaS offers processing, storage and other computing resources where the user is able to deploy and run operating systems and applications in the provider's infrastructure.[17] For instance, if there is Microsoft Office Word in your computer but not any free memory left, IaaS allows you to save or edit your document while it is in provider's storage. The customer has control over operating systems, and deployed applications (Microsoft

[12] Meil (2009) p.1

[13] Jadhwanl (2009) p.3

[14] Marchini (2010) p.5

[15] Jadhwanl (2009) p.3

[16] Hon (2011a) p.6

[17] Jadhwanl (2009) p.3

Word in the example) but not on the underlying cloud infrastructure.[18] For example Amazon's Simple Storage Service (Amazon S3) provides cloud storage.[19]

2.2.3 Platform as a Service (PaaS)

PaaS is an IaaS with added value designed to allow smaller providers to setup SaaS services quickly and cheaply.[20] In this case**,** you want special word software for your company and you have the expertise but not the tools, PaaS allows you to develop that special word software with the provider's development tools plus the infrastructure to offer that software as SaaS to other companies.

The customer has control over the deployed applications (the special word software) and possibly application hosting environment configurations but not the underlying cloud infrastructures.[21] For example Google App engine.[22]

The above service models may be viewed as a continuum, from low-level functionality (IaaS) to high-level functionality (SaaS), with PaaS in the middle.[23] The higher the functionality layer the higher the provider has control over the technology and thus, higher abstraction within that technology.

2.3 Deployment Models

Based on the addressee to whom it is deployed, cloud can be:

2.3.1 Public Cloud

Public cloud is a cloud service that is available for anyone willing to use it. The main virtues of such cloud are its ability to capture diversification of benefits and lower cost

---

[18] Jadhwanl (2009) p.3

[19] Marchini (2010) p.5

[20] Ibid

[21] Jadhwanl (2009) p.4

[22] Marchini (2010) p.5

[23] Hon (2011a) p.7

due to demand aggregation and multi-tenancy effect.[24] Security issues are the main associated concerns with such clouds.

2.3.2 Private Cloud

Private cloud is the cloud infrastructure operated solely for an organization.[25] Security concerns are less in private clouds. This is because they are easier to bring within the corporate firewall with less regulatory complications.[26]

2.3.3 Community Cloud

This is a cloud service used by a specific group of persons or a particular community that have shared concerns (e.g., mission, security requirements).[27]

2.3.4 Hybrid Cloud

A hybrid cloud is when an organization uses more than one type of cloud (public, private, or community) or more than one offering from different cloud providers.[28]

But there are sometimes references to consumer cloud (e.g. Facebook) as fifth model.[29] However, this can be embraced under public cloud category, as consumers are part of the general public.

2.4 Benefits of Cloud Computing

As cloud computing continues to unfold, the following are the benefits that can be attributable.

---

[24] Microsoft (2010) p.15

[25] Jadhwanl (2009) p.4

[26] Microsoft (2010) p.15

[27] Jadhwanl (2009) p.4

[28] Marchini (2010) p.8

[29] Ibid

1. *Cost saving*: cloud computing reduces the cost of acquiring and maintaining computing power by enabling agencies to purchase only the computing services they need, instead of investing in complex and expensive IT infrastructures.[30] Cloud computing offers services priced in terms of pay-as-you-go basis. The multi-tenancy nature of public clouds also lowers per-unit cost for providers.
2. *Immediacy:* is the ability to get and utilize a service in short period.[31] This facilitates completion of tasks in shorter time with less risk and lower administrative overhead than previously possible.
3. *Scalability and capacity:* scalability is the flexibility and easiness to change a demand in IT needs without major capital investments. Capacity can be added or removed in a very short period of time in support of a needed or unneeded mission.[32]
4. *Efficiency and resource maximization:* cloud computing cuts the resource on 'keeping the lights on' and freed significant resources that can be redirected to innovation, research and development. It can also fill up shortage of IT expertise.
5. *Security and reliability:* against the background that cloud is fraught with security concerns is the assertion that cloud can enhance security and reliability. The increased need for security and reliability leads to economies of scale due to largely fixed level of investment required in achieving operational security and reliability.[33] Large commercial clouds, with huge financial muscle are better placed to make cloud secure and reliable than an IT department in a corporation.

[30] Jadhwanl (2009) p.4

[31] Ibid

[32] Ibid

[33] Microsoft (2010) p.5

3 Chapter Three: Privacy in the Cloud

3.1 Privacy Defined

The term privacy is filled with definitional haziness. Such haziness relates to its *status* as a right or claim or form of control and its *characteristics*: is it related to information, to autonomy, to personal identity, to physical access.[34] Bygrave has summarized the various definitions of privacy in to four categories. Privacy in terms of:

- *non-interference (the right 'to be let alone')*
- *limited accessibility (the extent that we are known, accessible and subject to the attention of others)*
- *information control (power to control the flow of the information about self)*
- *an intimate* or *sensitive* aspect of persons' lives *(the state of control over intimate matters).* [35]

As mentioned above this paper is tailored to substantiate privacy issues in relation to cloud in light of EUDPD. The directive requires compliance to certain principles (e.g. fair and lawful processing, processing for specific-purpose) in case of *processing personal data* of individuals. Such protection of personal data can be encompassed as one aspect of the right to privacy. It is this kind of privacy as also called *Informational privacy* that data protection laws protect. Consequently, it has been claimed that definitions of privacy "in terms of information control tend to be most popular in discourse dealing directly with law and policy on data protection".[36] A reference to data

[34] Gavison (1980) p.424

[35] Bygrave (2010) p.170

[36] Ibid

protection law is to the rules that regulate the manner personal information is collected, registered, stored, and disseminated.[37]

The EUDPD, which dates back to 1995, was enacted without cloud computing in mind. The directive is currently being reviewed and there are indications that the ongoing revision will address the implications of such technology.[38] This and the following chapter will substantiate some of the privacy concerns that cloud computing have brought.

3.2 Personal data in the cloud

The starting point for a discussion on data protection laws begins with understanding the concept of 'personal' data. The EUDPD defines personal data as:

> *"Any information relating to an identified or identifiable natural person...; an identifiable person is one who can be identified, directly or indirectly..."*[39]

Identifiability is the main criterion that determines whether information is personal or not. Recital 26 of the directive lays down the criteria for identifiability.

> *"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."*

Two points worth noting in this recital. First is the term 'likely reasonably'. The duo introduces two criteria for identifiability: the term 'likely' referring to 'probability' of identification and the term 'reasonably' referring to the 'difficulty' in identification, in

---

[37] Bygrave (2002) p.2

[38] Kroes (2010) SPEECH/10/686

[39] Article 2(a)

terms of time and resource for instance.[40] The second point relates to a situation where certain information is rendered 'non-personal' through anonymization in which case the directive doesn't apply. However the heavy reliance of the directive's application on categorization of information as 'personal' is prone to criticism. It is "all or nothing approach: there is no room for 'more or less personal' data (and accordingly 'more or less protection')".[41]

Data being rendered anonymous means that information which ceases to be, 'personal data', may be processed in the cloud, without any need of compliance to legal requirements in the directive including the restrictions on transfers of personal data outside the EEA.[42] Pseudonymization and encryption can also be used to render information non-personal.

3.2.1 Anonymization and Pseudonymization

Anonymization is a process by which information is manipulated (concealed or hidden) to make it difficult to identify data subjects.[43] This can be done either by deleting or omitting 'identifying details' or aggregating information.[44] Whereas pseudonymization involves replacing names or other direct identifiers with codes or numbers.[45] Despite the term 'processing' within the directive is wide enough to cover the process of anonymizing/pseudonymizing in itself, it has been argued that to do so would be against the protection of individuals' privacy right, which is the main objective in the directive.[46] Thus, a purposive interpretation, which is also well recognized in the ECJ's jurisprudence, has to be called to exclude such process from being considered as 'processing'.[47] This is also because the underlying privacy interests are not threatened

---

[40] Bygrave (2002) p.44

[41] Robinson (2009) p.26-27

[42] Hon (2011a) p.8

[43] Ohm (2010) p.1707

[44] Hon (2011a) p.15

[45] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data,* 2007 (*WP136)* p.18

[46] Walden (2002) p.228

[47] Walden (2002) p.228-235

by such process and any other approach will discourage their use as privacy enhancing techniques.[48] Its impact on the widespread use of cross-border cloud services might not also be minimal.

If data is anonymized to the effect that it is no longer possible to associate to an individual (e.g. by irreversible anonymization) it will not constitute personal data.[49] Similarly as long as it is not possible to back-track an individual from pseudonymized data, it should not be considered 'personal'. The Article 29 Working Party (established under EUDPD Article 20 with an advisory role, hereinafter A29WP)[50] also considers irretraceable pseudonymized data as non-personal.[51] With regard to anonymization that can be retraced from certain indirect identifiers, the *'all means likely reasonably'* test provided in recital 26 has to be applied.[52] Accordingly, if it is not reasonably possible, with regard to time, expense and labor, to associate a data to certain individual, then the data remains non-personal. But once associated, it doesn't exclude the application of the data protection principles again.[53]

The same goes with key-coded data (pseudonymized data that leaves certain indirect identifiers). It has been asserted that if all appropriate technical measures are in place that prevents identification from happening under any circumstance, key-coded data may not be personal.[54] The European Commission has also held, in its Frequently Asked Questions (FAQs), that transfer of key-coded data outside EU without transferring or revealing the key does not involve transfer of personal data.[55]

---

[48] Hon (2011a) p.15

[49] EUDPD Recital 26

[50] The non-binding nature of its opinion will not guarantee that it will be followed and applied consistently across member states. Nevertheless, it remains helpful and pragmatic for the discussion at hand.

[51] WP136 p.18

[52] Casabona (2004) p.42

[53] Ibid

[54] WP136 p.18

[55] Hon (2011a) p.20

It should also be noted that whether information is 'personal data' or not is a question of fact, depending on the context.[56] Hence, anonymized/pseudonymized information which is personal data in one person's hand (e.g. cloud user) is not necessarily personal in the hands of another (e.g. cloud provider).[57] It all depends on all the available means that reasonably allow the data beholder to associate the information to an individual.

Hence, irretraceable anonymized and pseudonymized information can be processed by cloud providers without the need to adhere to the legal requirements under EUDPD. But an account of all the means reasonable to associate should be taken with regard to retraceable anonymized and pseudonymized information.

3.2.2 Encryption

Encryption involves the process of changing a plain text in to unintelligible code.[58] While decryption is reversing back the unintelligible code in to readable text. Cryptography, often used interchangeably with encryption, is the related science dealing with the technicalities of creating encrypted information.[59] The discussion on whether the process of anonymization/pseudonymization constitutes 'processing' also applies for encryption. Despite encryption's paramount importance for cloud computing its fuller exhaustion of the technology is hindered by the legal restrictions on the import, export and use of encryption in different jurisdictions.[60]

Encryption is not explicitly recognized within the directive. But at the crux of recital 26 is the effect rather than the method used. Thus, if information is encrypted in such a way that is no longer possible to identify the individual, it is not personal data. This seems also to be the opinion of the A29WP which considers that 1 way cryptography (irreversibly encrypted data) would not constitute personal data as long as it is

[56] WP136 p.13

[57] Hon (2011a) p.14

[58] Comment (1997) p.1405

[59] Perkins (2005) p.1628

[60] Kuner (1996) p.186

effective.[61] However, the impossibility should be understood in relation to the 'likely reasonably' test discussed above. Such test doesn't require an absolute impossibility as well as doesn't encompass accidental matching. The assessment is also context dependent. Accordingly, even an irreversibly encrypted data in the hands of the cloud user doesn't guarantee it is non-personal in the providers' hand considering the resources and other information the later can employ to identify the individual.

Nevertheless, the need for later use of the data by cloud users makes reversible encryption more relevant to cloud computing than irreversible encryption. Despite this the A29WP didn't address the status of such data. But there are claims that if a key-coded data that leaves some information accessible is non-personal *a fortiori* an encrypted data which is completely transformed in to another form poses fewer risks and should not be personal.[62] The effectiveness of the encryption remains relevant in such a case also.

Three factors affecting the strength of encryption are key-security (how securely the key is handled), underlying algorithm (whether the encryption is based on well established algorithm) and length of the key (the longer the key the more likely secure against attacks).[63] Thus, if a cloud user encrypts a data with strong encryption algorithm, strong encryption key and kept the key secure, the data may not be personal in the hands of the provider.

Other factors such as the kind of information, duration of encryption, the potential receivers and the resources they have can affect the appropriateness of an encryption. [64] Accordingly, a data 'in motion' can be rendered non-personal by less powerful encryption than a data in long-term storage.[65] Furthermore, the fact that Article 25 of EUDPD recognizes duration of processing (as a criterion in assessing adequacy of

---

[61] WP136 p.20

[62] Hon (2011a) p.25

[63] Perkins (2005) p.1629

[64] Ibid

[65] Hon (2011a) p.27

countries) implies that less stringent requirement may be followed when data is exposed to short period of processing in third country.[66] Similarly, the fact that a data is exposed unencrypted for short period shouldn't make the data personal.[67]

Thus, a data which is placed encrypted in the cloud can be decrypted and processed while in the provider's control without that data becoming 'personal' provided that the duration it stayed unencrypted is short. However, such short exposure should not be overlooked as some providers of SaaS can catch a copy during that interval. Accordingly, whether the provider' role is limited to mere provision of infrastructure or have active role in processing should be considered together.

3.2.3 Data of Legal persons in the Cloud

Personal data, as defined in Article 2(a) of the EUDPD relates to information concerning natural person. This, together with lack of extending the protection to data of legal persons in many member states has been claimed as creating reluctance on the part of companies to stock their confidential information (e.g. know-how, industrial secrets, etc) or using the cloud for communication purposes.[68] Such lack of protection can leave companies in the member states lacking protection at competitive disadvantage. It could particularly "compel Small and Medium-sized Enterprises (SMEs) and non-profit organizations to contract under unfavorable conditions, having less regards for data protection and privacy".[69]

However, the interpretation by Strasbourg Court of Article 8 of European Charter of Human Rights (ECHR) in a way that protects not only the individuals but also legal persons notably their industrial secrets, knowhow, etc can be taken as a positive move towards curtailing such a problem.[70] Furthermore, the Directive on Privacy and

---

[66] Ibid

[67] Ibid

[68] Poullet (2011) p.389

[69] Poullet (2011) p.388

[70] See Poullet (2011) p.388

Electronic Communications[71] has opened a leeway for extension of protection to legal persons which can be taken as trendsetter in the area. But such extension can raise variety of questions,[72] which calls for cautious approach in answering 'how' to extend the protection.

3.3 Controller Vs Processor distinction in the Cloud

The 'controller-processor' distinction is vital in the EUDPD as the duties and responsibilities are mainly imposed upon designating a party as 'controller'. 'Controller' is "…natural or legal person… which alone or jointly with others determines the purpose and means of processing of personal data..."[73] While 'processor' is '…natural or legal person…which processes personal data on behalf of the controller...'[74] The distinction lies on the determination of purpose and means of processing.

The A29WP has established that one who determines the purpose or the effective means of processing qualifies as controller.[75] The 'effective means' criteria reduced the role of the controller in determining the 'means' only to those that involve 'substantial' questions 'which are essential to the core of lawfulness of processing' and gives a 'margin of maneuver' for processors to determine technical and organizational questions without being considered 'controllers'.[76] Despite this, the categorization remains quite difficult. More particularly the cloud is blurring such a distinction due to plethora of chain of actors with differing and mixed responsibilities changing over time.

Are cloud providers then data controllers or data processors?

---

[71] E-privacy Directive 2002/58, Recital 7

[72] Kuner (2007) p.77

[73] EUDPD Article 2(d)

[74] EUDPD Article 2(e)

[75] Article 29 Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor'*, 2010 (WP169) p.13

[76] WP169 p.14-15

Here a distinction need be made between user related and cloud-processed personal data.[77] The former refers to the data provided by the customer when subscribing to the service and usage generated data, while cloud-processed data refers to data of other individuals, stored or otherwise processed by the user in the cloud.[78] It is lucid that the provider is a controller with regard to user related data as it determines what data to collect and why. But ambiguities remain with regard to cloud-processed data.

It has been asserted that the factual circumstance is most relevant than 'fine tune' designation based on contract or law.[79] Thus, whether cloud provider is processor or controller, with regard to cloud-processed data, depends on the assessment of particular circumstance. For example, the extent of control the customer has, the kind of service provided and other facts. The main question remains "to define who is who and who does what".[80] Despite some differences, the widely held view is to consider cloud providers as processors of such data unless processed for the provider's own purpose.[81] All, however, remains same in their attempt to categorize cloud providers to either controller or processor.

A more deviant approach has been introduced by Professor Ian Walden and others in their recent treatise to hold that only when the provider 'crosses the line', by processing the data for its own purpose or allowing unauthorized third party access, should be treated as 'controller'.[82] The situation with most Social Networking Sites falls under such category.[83] In most other cases the provider is neither controller nor processor.

The authors then suggested two proposals for better protection of individuals' privacy rights. Firstly, abolishing the 'binary' controller-processor distinction and introducing end-to-end accountability that may impose primary liability on one party, but assign

---

[77] Hon (2011b) p.11

[78] Ibid

[79] WP169 p.15

[80] Poullet (2011) p.389

[81] Ibid see also Hon (2011b) p.14

[82] Hon (2011b) p.21

[83] Ibid

different degrees of responsibility and liability to other actors in proportion to their role in the chain.[84] Secondly, an introduction of neutral intermediary liability regime of the E-commerce Directive (ECD) based on knowledge and control of data.[85]

Though the above approach is such innovative and potentially fosters cloud computing, there are some points that need consideration. First, suggesting that different degrees of responsibilities should be assigned according to the role of actors involved seems to lay a formidable task on the legislator to foresee possible players in cloud-chain. This will be particularly problematic, having regard to the alarming rate of IT growth.

Second, though the attempt to exempt cloud providers from being 'controllers' can be justified by the heavy responsibilities attached to it, it is hard to see any benefit from same move with regard to 'processor'. The only duty attached to a 'processor' is to take appropriate technical and organizational security measures and follow instructions of controller.[86] In case of contractual obligations, it is subject to bargain and is based upon will. The fact that cloud provider is not a processor will not relive it from such obligation. This is because, the provider must, for commercial reasons, follow instructions of its customers and take appropriate security measures.[87] Thus, the move doesn't payoff significantly for the provider. Further the ECD intermediary liability regime rather adds complications associated with 'knowledge' element. However, the introduction of intermediary liability can be considered as an additional measure to assess the liability of processors in case of failure to comply with their obligation.

Even a claim that such move could possible relieve from complying with the provisions restricting transfer of data outside EEA (because it is the user who is controlling the whole operation) is hardly sustainable. This is because the provider's unawareness as to nature of the data and its lack of involvement in processing doesn't avoid the risk of access by third parties (e.g. governments) in the place of storage, unless there are

[84] Hon (2011b) p.24

[85] Ibid

[86] EUDPD Article 17

[87] Marchini (2010) p.62

technical measures in place. Finally, it seems rather illusive, with the term 'processing' defined so widely, for national DPAs to sustain that cloud providers are not at least 'processors'.

3.4 Cloud Contracts: overview of some Terms and Conditions with privacy implications

3.4.1 Amendment of Terms and Conditions

A survey covering 27 providers has revealed 13 of them have reserved the right to unilaterally amend the terms simply by posting an updated version in their website, with only four having undertaken to notify through different mechanisms.[88] Provider Zecter's terms for its service ZumoDrive stipulates the right to update and change terms and conditions without notice and a continued use of the service after such change to constitute consent to the changes.[89]

This shows majority of the providers does not take any positive action to notify the user that change has been made to the terms. This requires users to regularly review terms and conditions. In Europe 'consumer' users (non-businesses) of cloud are protected by the Unfair Contracts Term Directive (UCTD)[90], though such changes can sometimes have serious implications. [91] For instance, a change on single term can be decisive on the legality of their move to the cloud (e.g. change in the location of the data). Thus users from such jurisdictions should pay serious attention to such policies of providers.

3.4.2 Choice of Jurisdiction and applicable law

The same survey has uncovered most providers stipulate the application of a law and a court of jurisdiction in which they have principal business place, with short period of

[88] Bradshaw (2010) p.21

[89] Ibid

[90] Unfair Contract Term Directive 93/13

[91] Svantesson (2010a) p.395

limitation to institute a claim.[92] For instance, Amazon chose Washington law as governing law with ADrive requiring claims to be instituted within 6 months.[93]

Despite this, European consumers (non-business cloud users) can get rid of such clauses by availing the Rome I[94] and the UCTD.[95] Article 6 of Rome I stipulates for the application of consumers domicile law in case of claims arising from contractual obligations. Whereas the UCTD Article 3 excludes the application of 'unfair' terms on consumer contract i.e. terms not individually negotiated and that causes a significant imbalance to the detriment of the consumer are regarded as unenforceable. From the non-exhaustive list of 'unfair' terms in the Annex of the directive, sub-paragraph (q) can be used as a loophole for the exclusion of the application of such clauses.

3.4.3 Exclusion of Liability

Most providers seek to exclude liability for damage resulting to the customer. For instance, Google disclaims liability for its service Google Apps, "the services seek might be interrupted, untimely, insecure, full of errors…, but …you expressly agree that Google and partners shall not be liable to you for any direct, indirect… damages resulting from any matter relating to Google Services".[96]

Arguably such exclusions may not be unreasonable. The multi-tenancy of such services means multiple losses can be suffered by users. If passed to the providers; they can reach a level to jeopardize the existence of the provider.[97] Such a manifestation is hardly conceivable though when it relates to failure to provide the particular services that users require. European 'consumers' can still get shield of the UCTD. In the UK, the Unfair Contracts Act 1977 protects not only 'consumers' but also 'businesses' from

[92] Bradshaw (2010) p.17-18

[93] Ibid

[94] Regulation 593/2008/EC

[95] Unfair Contract Terms Directive 93/13

[96] Mowbray (2009) p.137

[97] Marchini (2010) p.133

such clauses.[98] The protective approach in Europe has resulted in such distinction that providers in Europe are less overt to exclude liability than their US counterparts.[99] Despite this, customers using the cloud particularly to store or process 'sensitive' personal data should take precautionary approach than relying on the reactive provisions. This advice is all the poignant given that it is also not easy to identify the party responsible in a case of breach.

3.5 Data Ownership and its implication for privacy in the cloud

Ownership of information is used in this section in the sense that information can be an object of right derived from laws such as Intellectual property (IP), Privacy and Law of Confidence. Information is the main commodity in the cloud. Issues arise as to ownership of data within the cloud, and to which data such ownership refers. For this purpose, distinction needs to be made between cloud processed data and cloud generated data.[100] To tailor the discussion to the case of personal data let's assume a customer has entrusted the personal data of its employees in to the cloud. Then the issues that emerge are:

1. Whether the customer can claim an ownership right over cloud-processed data?
2. Who has ownership over the cloud-generated data?
3. Can generation of the data by the provider interfere with ownership rights of the customer, if any? and
4. Can creditors (e.g. sub-contractors) of the provider attach a customer data as an asset, in case the provider goes bankrupt? What about cloud generated data?

It is worth noting that ownership issues in 'personal' data of individuals entrusted to consumer clouds by themselves is omitted from this discussion as it raises a difficult philosophical question of whether ownership right should exist over personal data as such, which goes beyond the reach of this paper.

---

[98] Marchini (2010) p.129

[99] Bradshaw (2010) p.41

[100] See above (n 78)

IP law, law of confidence or contract law plays an important role in determining the first question.[101] Apropos IP right, the analysis is founded upon whether the employees' personal data can qualify for IP protection based on how such data is organized. For instance, if the data is organized in such a manner as to show, apart from the personal details, the performance results of each employee, and other data, there is possibility that it can qualify as literary work in signatories of Bern Convention. But if the data in the cloud contains only pure personal details, IP law may not be helpful. However, at least in Europe, it can qualify as *Sui generis* database right as far as they pass the 'substantial investment' test.[102] Nonetheless the ECJ's interpretation that the 'substantial investment' should be directed towards the creation of the database than collection seems to hinder its potential use in protecting data in the cloud.[103] Even assuming that the data is protected either by IP or *Sui generis*, it has little relevance for data protection purposes. This is because IP law and even worse *Sui generis* does only prohibit certain kinds of uses by third parties. Such use as permitted by the laws could have huge negative privacy ramifications.

The other relevant area of law is law of confidence. Article 39(2) of TRIPS has set three criteria for information to be protected under such law.[104] The information must be (a) secret, (b) has commercial value because it is secret and (c) reasonable steps to keep it secret are taken by the person legally in control of the information.[105] Despite difficulties for personal data, particularly pure personal details to fulfill such requirements, in case it does, law of confidence is more effective than IP law for data protection purposes. This is because it absolutely shields against disclosure by the provider to third parties, in the absence of third party disclosure principle, as in the US. To a lesser extent, it also protects against the provider's own use when the provider

[101] Reed (2010) p.10

[102] Database Directive 96/9, Article 7(1)

[103] Case C-203/02 [2005] ECDR 1

[104] Reed (2010) p.11-12

[105] Ibid

takes unfair advantage.[106] But it must not be ruled out that the 'not-unfair' use by the provider could sometimes risk the privacy of the data subjects.

Finally, contract law plays crucial role in determining ownership rights by clarifying the copyright and confidentiality relationships in the terms of service for the cloud computing.[107]

With regard to the ownership of data generated in the cloud, second question, either by the customer or provider, the same line of assessment as above has to be made.

Thus, if ownership over data exists as above, the generation of data by the provider possibly violates the law based upon which the ownership is claimed. If ownership flows from IP law, then copying, even temporarily, without license to generate such data violates the IP right of the customer.[108] In the same vein, copyright can restrict the replication of data in to different machines that deprives the efficiency of cloud services. If ownership flows from law of confidence, disclosure to third party will violate such law.[109] This implies an IP right over data in the cloud can avoid data mining or profiling while ownership flowing from law of confidence avoids disclosure to third party, which is at the heart of the interests that data protection laws are intended to protect.

Little has been said about the attachment of data by creditors. With regard to cloud-processed data, it is less likely that creditors will have any claim over such data. Such data has already an established ownership status before going to the cloud and the mere placing of it in to cloud shouldn't change that status.[110] The practice complements this in that a survey of providers reveals that there is no provider claiming ownership and proprietary right over the content placed in the cloud.[111] Thus, it can be argued, if the

---

[106] Reed (2010) p.18

[107] Reed (2010) p.13

[108] Reed (2010) p.19

[109] Reed (2010) p.17-19

[110] Reed (2010) p.6

[111] Bradshaw (2010) p.31-32

provider doesn't have legitimate claim over cloud-processed data, neither do the creditors.

With regard to attaching of cloud-generated data, it is strikingly difficult to answer. Nonetheless, it seems of little privacy risk if creditors' can attach anonymized data legally (from both data protection and contract law perspectives) generated by the provider which has commercial value, if all adequate technical and organizational measures were taken when anonymizing.

3.6 Other privacy issues in the cloud

***Lock-in and portability*:** it is easy, perhaps too easy[112] to find your way to the cloud, but never the same to get out. Such a problem, known also as lock-in, refers to the difficulty in moving data between providers or cloud services or else to pull-back the data where the relationship with the provider is terminated. The main concern of customers, according to survey, is the possibility of being locked-in with the provider.[113] Lack of standardized data formats or service interfaces or the incentive of the provider not to let-go its customers can be reasons for lock-in.[114] Lock-in can lead to serious data loss due to inability to retrieve it easily in case acute danger to the security of the provider is imminent.

Notwithstanding this, portability can be a problem by itself. This is the case where unintended privacy harms can result when consumers pull information about others in to less protected spaces and to providers with different policy and privacy norms.[115] Developing an industry standard and transparency within providers can be the way forward for such problems.

***Profiling and Data mining*:** despite difficulties in distinguishing the two concepts, it seems profiling has a wider reach than data mining. Profiling is the process of

---

[112] Chow (2009) p.87

[113] Mowbray (2009) p.142

[114] Catteddu (2009) p.25

[115] Pew Internet (2010) p.17

knowledge discovery in databases with regard to any kind of information that makes a difference in decision making about an individual while data mining is only based on pre-defined class of information.[116] A profiler sketches the individual with respect to any information (likings, disliking, what he knows, what he doesn't, etc) deemed to be relevant but data miner sketches the individual with respect to predefined set of information (only what he likes).

The cloud has tremendously enlarged the potential for profiling and data mining. First; it gave attackers massive centralized databases for analysis and computing power to that end and second, it also opened the possibility for profiling and data mining by the provider's themselves.[117] Google's term of service, for instance, has recognized the possibility for Google combing information from its different services.[118] This has significant privacy ramification. The ubiquity of profiling and data mining, as Lessing has succinctly noted, has shifted the burden of proving the profiled person innocent, as it provides governments even evidence of criminal intent.[119] Overleaf, profiling brought with it free or cheap services and there are even claims that profiling enhances privacy as it enables the profiler to interfere only when it is relevant to us.

Transparency, 'privacy-by-design' and introducing the right of access to profiles are some of the future forwards promoted to address such problems. But the astounding development of profiling technologies remains a challenge to the bite of such measures.

---

[116] Hildebrandt (2009) p.239

[117] Chow (2009) p.88

[118] Svantesson (2010a) p.394

[119] Lessing (2006) p.205

4 Chapter Four: Cross-border data flow regulation in the Cloud: EU perspective

4.1 Cross-border data flow

4.1.1 Rational for Cross-border data regulation

The term cross-border relates to where the data subject is located in a different country from the data controller, the data itself has passed to a third country, or simply important evidence is located in a third country.[120] "Preventing circumvention of national data protection and privacy laws; guarding against data processing risks in other countries; addressing difficulties in asserting data protection and privacy rights abroad; and enhancing the confidence of consumers and individuals" are claimed to be the four main policy motivations for regulating cross-border data flows.[121] But with the OECD (Organization for Economic Cooperation and Development) guidelines, the motivation was to avoid the barrier to free flow of data due to competing national privacy laws.[122]

The fact that cloud computing has eased the way data transfers and the difficulty of determining location of data has posed stiff challenge to the traditional 'point-to-point' based cross-border regulation. This makes imperative to revisit most cross-border data regulation legislations for the efficient use of cloud services with utmost regulatory efficiency.

4.1.2 Geographical Vs Organizational approaches to Regulation

Geographical-based approach, which is based on 'adequacy' assessment in foreign jurisdictions (e.g. the case in the EUDPD) aims to protect against risks posed by the

[120] OECD (2006) p.20

[121] Kuner (2010a) p.6

[122] OECD (2006) p.6

country or location to which the data are to be transferred regardless of who the receiver of the data in that country is.[123]

Organizational approach, which is based on 'accountability' principle (e.g. Asia-Pacific Economic Cooperation (APEC) privacy framework), on the other hand, aims at managing the risks that can be posed by receiver of the data and focuses on making the transferor accountable regardless of where the receiver of the data is located.[124] However, a mix of the above approaches is also possible as in the EU legal framework where the adequacy approach is combined with the use of Binding Corporate Rules (BCRs) and Standard contractual clauses having the nature of organizational approach.[125]

4.2 EU regime on transfer of personal data outside EEA: General overview

Chapter IV of the EUDPD deals with transfer of personal data to third countries. Article 25(1) of the directive, adopting the 'adequacy' approach, restricts flow of data from EEA to any country except those that ensure 'adequate protection'. The Commission has identified Argentina, Canada, the Bailiwick of Guernsey, the Isle of Man, and Switzerland as adequate countries.[126]

For all the other countries, the transfer is only possible either by using the exceptions under Article 26(1) or by taking 'adequate safeguards' as per Article 26(2) including the US Safe Harbor Agreement. Put in terms of hierarchical legal preference, the adequacy method under Article 25 is at the top followed by the 'adequate safeguards' method under Article 26(2), then use of the exceptions in the bottom.[127] This is because the degree of protection slides down from top with adequate protection in the whole country, to the middle only in the particular organization, with no protection in the bottom of the hierarchy. Restrictions on transfer can, nonetheless, exist even where a

[123] Kuner (2010a) p.28

[124] Ibid

[125] Ibid

[126] Kuner (2007) p.174

[127] Kuner (2007) p.158

country is assessed adequate or between EU member states on legal ground other than the lack of adequate protection.[128]

Notwithstanding this, the regime has been subject of many critics. One such criticism emanates from the regime's highly labor and capital intensive nature, this being the reason only small and handful countries has yet managed to get the adequacy stamp.[129] Failure to regulate onward transfer (re-exporting data from the original destination to another country) is also another criticism. Though the A29WP opinion has filled the gap, its non-binding nature creates uncertainties in its practical implementation.

Furthermore, the use of the term 'third-country' in Article 25 creates a loophole of non-regulation when data is transferred to non-country destinations i.e. to international spaces such as high seas.[130] Though looks far-fetched, it is not unrealistic as Google is already pursuing to establish offshore data storage centers.[131] This being also the reason a reference to the term 'cross-border' is preferred over 'transborder' in this paper, as the former is destination neutral.

The cloud has exacerbated such problems. This is because the adequacy test requires ascertaining the location and the receiver of the data which is formidable task in the cloud due to its architecture. Some providers have begun data zoning, locating a data from European customer in Europe, but even in such cases there are reliability questions.[132] It also reduces the efficiency of the cloud. The problem is worse in the Web 2.0 age, where individuals are not even aware that they are transferring data when they upload personal information in to servers of social networking sites located outside EEA.

---

[128] Kuner (2007) p.153

[129] Kuner (2009) p.263

[130] Svantesson (2010b) p.7

[131] Ibid

[132] Hon (2011c) p.8

The accountability approach has been promoted firmly as way forward.[133] The European Commission has also confirmed that it is considering this approach in the ongoing review of the directive.[134] Despite ensuring easy redress to data subjects (by making the exporter accountable) such an approach is also fraught with its own inherent problems. It lays the burden of proof on the individual on breach and damage issues which is difficult task in cross-border cloud services.[135] Thus a total shift in the approach may lead to undesirable result which is well described as a move "from a weak regime aimed at preventing harm, to an unrealistic and naive hope of correcting harm after it occurs".[136] Hence it is important for the legislature to find the balance between the two approaches for better protection of personal data.

4.3 Does Cloud Computing involve cross-border data flow?

At the starting point for such a discussion is the note that cloud computing is an evolving technology that is not possible to depict fully how it works. Various other factors such as the type of cloud, type of data, status and perhaps knowledge of the parties can affect the assessment of when cloud computing trigger the cross-border rules. This section will try to identify and discuss the factors that can/should have determinative values in deciding whether use of cloud services involve cross-border flow of personal data.

Further the point-to-point transfer assumption, within the EUDPD, is in a diametrical contradiction with cloud computing that contemplates the transferring of data to myriad of locations across different jurisdictions. This also made this discussion difficult. How, for instance, the restrictions on transfer will be applied in case personal data is processed in servers of a provider located in countries that ensured adequate protection and those that do not, with the data continuously changing between these servers?

---

[133] Kuner (2009) p.269-272

[134] Reding (2011) p.4

[135] Svantesson (2010b) p.10

[136] Svantesson (2010b) p.9

That aside, distinction need first be made between domestic and cross-border cloud services for the purpose of this discussion.[137] In domestic clouds the whole processing is located in one jurisdiction.[138] In such clouds there is normally no cross-border issues as the data remains in the same territory. But the second type of cloud services seems to raise issues of cross-border flow of data as it involves different jurisdictions.

Nevertheless, whether a data is transferred from cloud-user to provider (or between providers) and within the same provider can sometimes result in different consequences. A prominent example is the current Australian privacy legislation. The National Privacy Principle 9, regulating cross-border flow of personal data, defines the receiver as someone '*other than the organization or the individual'*.[139] Thus, transfer of data even across different jurisdictions, by an organization, about an individual to that individual himself or within that organization, doesn't amount to cross-border transfer of data. Indeed, the transfer of a personal data about an individual to that individual doesn't normally raise any privacy issues. This may not, however, always ring true. Take, for e.g., Australian doctor sending to Australian client medical results via e-mail with the e-mail that contains such sensitive personal information stored on servers abroad.[140] There is clearly an apparent privacy risk of access by third parties in such situation. The same risk exists when the transfer is within an organization but to subsidiary outside the jurisdiction. The existence of such risk along with the non-existence of a term like in the Australian legislation, within the EUDPD, can generally be taken to mean transfer of personal data even within an organization will constitute cross-border transfer of data.

With regard to the data transfer from cloud user to provider/between providers, there are claims that cloud-based processing with providers outside Europe constitutes cross-

[137] Svantesson (2010a) p.392

[138] Ibid

[139] Svantesson (2010a) p.393

[140] Svantesson (2010b) p.12

border transfer of data and can't even be justified within the exceptions.[141] But such a conclusion seems to overlook many factors on a particular cloud service.

One such factor is the location of the data. Even if the provider is established outside EEA, if it undertakes to process/store the data within EEA, there is no reason, in normal circumstance, to consider it as cross-border transfer of data, as the data never transcends any border. But other factors can influence such a position. For instance, the Amazon S3 storage service lets customers choose to store the cloud-processed data in Europe, but it is not clear, from the S3 terms of service, whether or not cloud-generated data will be stored in Europe, if they make this choice.[142] It means there is no guarantee that such data will remain within EEA. In such cases if the provider reserves the right to monitor and profile the activities of the user, such factor should be given a considerable weight.

Imagine Amazon has already undertaken in its terms and conditions to store all cloud-processed and generated data within EEA. Amazon also reserved the right to unilaterally change the terms and conditions without notice to the user. Should this make a difference? At the very least, cautious approach is needed with regard to those providers who undertake zero steps to inform the change of the terms and infer consent from the continuing use of the service. It is because there is an apparent risk that the data can be without protection where Amazon decides to change the location of the data and the user consenting without being aware of the change. This sends the signal that cloud users should not be reliant only on the data zoning undertakings without thorough analysis of each terms of service.

Whether the service is IaaS, PaaS or SaaS and the appropriate security measures in place could also have a determinative role. It has been asserted above[143] that the providers' functionality in case of IaaS and PaaS is lower than in case of SaaS. Thus, where the data is sufficiently encrypted with all the appropriate safeguards against decryption, and with the providers' system allowing transmission and storage of such

---

[141] Weichert (2011) p.11

[142] Mowbray (2009) p.142

[143] See (n 23)

encrypted data, it is more probable that it will not constitute cross-border transfer of data to the IaaS or/and PaaS providers irrespective of the location of the data.

Such approach goes in line with the European Commission stance that transfer of key-coded data outside the EU without transferring or revealing the key does not involve transfer of personal data.[144] It may be hard to sustain in case of SaaS where data has to be decrypted for processing and the provider could access the data in order to deliver the service. Despite claims for processing data while encrypted,[145] such technologies may not help in case where the business model of the SaaS providers is totally dependent on having access to personal data, such as Facebook. After all, it will be a suicide to their business to allow encrypted processing, which they don't dare to do it.

This calls for adoption of flexible approach that allows case by case analysis considering the relevant factors. Reinforcing the use of pseudonymization and encryption measures by prescribing in terms of obligations on providers can also merit consideration.

4.4 Legal bases for using cross-border clouds

4.4.1 Legal bases other than consent

Recital 60 of EUDPD considers transferring of personal data outside EU as 'processing'.[146] This requires, besides compliance to the requirements of Articles 25 and 26, legalizing the processing as per Article 7 or 8 of the directive. Here it is assumed that controllers' motivation to use cross-border cloud service is cost and efficiency reasons. Such assumption reduces the possible legal grounds in to consent (both under Articles 7(a) and 8(2(a)) as discussed in section below), and 'processing necessary for the purposes of the legitimate interests pursued by the controller' (Article 7 (f)). With regard to the later, it has been claimed that firstly, at this moment there are no compelling grounds to use cross-border cloud due to adequate supply of cloud

[144] Hon (2011a) p.20

[145] Ruiter (2011) p.369

[146] Kuner (2007) p.159

services within EU and secondly, even where the non-EU services are less expensive and more efficient, cost and efficiency reasons will not reach the requirement of 'necessity'.[147] But where such saving and efficiency is of substantial, compared to EU cloud, it has been argued, such use can be justified.[148] This approach should be favored as such cost-saving can enhance protection, for instance by investing in adequate encryption technologies. Moreover, there is no risk to the data subject either.

This arises because, if there are interests or fundamental rights and freedoms of data subject that needs protection (Article 7(f)), data controllers can't justify the transfer on cost and efficiency reasons. Indeed, there are privacy concerns, to the data subject in the cloud (e.g. access by law enforcement authorities), that call for protection where his personal data is transferred to third country without adequate protection. Such concern can however be alleviated if adequate safeguards, such as encryption or sufficient anonymization/psedonymization, are in place.

Notwithstanding this, can transferring of data in to cross-border clouds for more security and reliability be justified as processing to protect the 'vital interest of data subject' as per Article 7(d)? For instance, where giant cloud providers such as Google have introduced advanced security protection measures that can't be afforded by most controllers. If the scope of 'vital interest' in this article is interpreted in the same manner as 'vital interest' under Article 26(1(d)), where it is only applicable in case of medical emergency to the data subject,[149] it would of little help.

Posit the controller is successful in justifying the processing (transfer to third country); it must also comply with the requirements which restrict transfer of data outside EEA. The first (and most preferred) method is to use a cloud service that involves processing of data in a country that ensures adequate protection pursuant to Article 25.

---

[147] Weichert (2011) p.6

[148] Weichert (2011) p.7

[149] *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC*, 2005 (WP114) p.15

The second preferred method involves making use of Article 26(2). This constitutes transferring data using the Standard contractual clauses, as approved by the Commission, or using BCRs or the US Safe Harbor.

The European Commission has already approved two kinds of standard contractual clauses regulating: (a) controller-to-controller and (b) controller-to-processor flow of personal data. However, such a distinction fits uneasily into the cloud, where there are many actors with no clear duties or with continuous change of tasks. Even worse, if there is situation, as claimed above[150] that cloud providers can be neither controllers nor processors, it means standard contractual clauses will not provide any legal basis for transferring data in to cross-border cloud services. The same problem is claimed to exist in using Safe Harbor where there are uncertainties whether a mere processor can join the agreement as the obligations are tailored for controllers.[151] Furthermore, the fact that cloud computing involves transfer of data to multiple actors across different jurisdictions can make the use of standard contracts bulky and time consuming. Besides, pursuant to Article 26(2) use of adhoc contracts (non-standard contracts) can be made to transfer data despite associated procedural and administrative difficulties.[152] The multi-actor and foggy role of actors in the cloud more complicates such procedural and administrative difficulties.

Use of BCRs has been promoted as better way for transferring data in to cross-border clouds,[153] though not without difficulty. It is because the A29WP has interpreted 'corporate group' as group of commercial entities which stand in ownership relationship to each other.[154] Bar rare situations, in typical cloud environment, providers' use resources and services of other providers with which they don't have any ownership connection. This hinders the use of BCRs. But BCRs remain ideal for multinational cloud providers operating in different jurisdictions. Nonetheless, it seems BCRs fall

---

[150] See accompanying text (n 82)

[151] Kuner (2007) p.182

[152] Kuner (2007) p.209

[153] Poullet (2011) p.397

[154] See in Kuner (2007) p.222

short of transferring data from controller-processor or processor-processor, which is mostly the case in the cloud, as against controller to controller.

Where the controller is not successful in using the above methods, it has to resort to the exceptions under Article 26(1). Similarly the assumption that transfer to third country is made for cost and efficiency reasons reduces the possible legal bases that can mainly be utilized in to:

- unambiguous consent of data subject (Article 26(1(a)) discussed next section)
- transfer is necessary for the performance of a contract between the data subject and the controller (Article 26(1(b))
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party (Article 26(1(c))

Nonetheless it seems possible to argue that the cost and efficiency reasons can constitute 'necessary for public interest' under the first alternative of Article 26(1(d)). In such a case whether there is substantial cost saving, what kind of public interest is pursued and other available alternatives may have relevance.

Though wider usage of sub-paragraph (b) to transfer data in to cross-border clouds seems possible, its utility is limited. The A29WP and DPAs has rejected claims that transferring employee data in to centralized Human Resource data base outside EEA for payment functions is not necessary for the performance of the employment contract between the data subject and employer as performance can be guaranteed '*without transferring'* the data outside EU.[155] This seems to imply that transferring data in to the cloud involving transfer to third country is necessary for performance of the contract if performance can't be made without outsourcing and by outsourcing to cloud within EU. But such situation seems more hypothetical than realistic.

[155] Kuner (2007) p.213-214 (emphasis added)

But it has been acknowledged that the cost-efficiency to the employer may '*indirectly benefit'* the employee.[156] It is doubtful if such acknowledgement can be taken to imply that a substantial cost benefit to the employer can be considered 'in the interest of the data subject' (Article 26(1(c)) as it may sometimes result in more than 'indirect benefit' to the employee.

This aside, can transferring data outside EEA for reasons of more security and reliability, as illustrated above be justified as processing to protect the 'vital interest of data subject' pursuant to Article 26(1(e))? Though A29WP has rejected same reasoning for outsourcing payrolls by employers,[157] it seems appropriate to allow such a transfer where the kind of data requires high degree of security such as financial data.[158] Thus, a search for more security can be claimed as to the interest of the data subject. However, the uncertainties over the security of the cloud and how it actually works can reduce the potential use of such argument.

As a general remark, with their associated difficulties, use of standard contractual clauses, Safe Harbor Agreement, '*adhoc'* contracts and BCRs remains preferable for companies to resort to compared to the exceptions.

4.4.2 Consent as a basis of transfer

The surfacing of the cloud has questioned the appropriateness of consent as an independent legal basis either for processing or transfer. Sometimes such challenge flows from the very architecture of cloud computing. For consent to be valid it should be freely given, specific and informed (Article 2(h)). Furthermore, Articles 7(a) and 26(1(a)) additionally requires the consent to be 'unambiguous' while Article 8(2(a)) requires consent to be 'explicit'.

---

[156] Kuner (2007) p.213-214 (emphasis added)

[157] Kuner (2007) p.214

[158] The failure to include financial data within the definition of 'sensitive personal information' has been raised as a draw-back within the directive.

The 'specificity' element requires for consent to be given to a precisely and clearly identified set of processing.[159] If the specific circumstances under which the processing will undergo are not known when consenting, consent is not valid.[160] However, in the cloud it is not possible to depict all the circumstance, such as the location of the data, to a required detail to make it 'specific'. But data zoning can mitigate such problem. Nonetheless, the 'specificity' element also requires the need for new consent if the purpose of the processing is changed at some point.[161] But the survey discussed above[162] shows that some providers have reserved the right to change the terms of services without even giving a notice to the data subject or cloud user and inferring consent from the continuous use of the service which is in clear contradiction with the 'specificity' requirement. It is because a change in one term of service can result in a change in the purpose of the processing that requires a new consent of the data subject or/and cloud user.

In addition, consent should be informed. This requires that the individual must be given in a clear and accurate manner interalia the relevant information regarding the purpose of the processing, the identity and details of recipients of possible transfer. [163] It seems unlikely that informed consent can be given in the cloud due to the uncertainty as to how data is processed and where it is being sent.[164] Furthermore, for consent to be informed the information given should be appropriate in terms of its quality, accessibility and visibility.[165] Accessibility and visibility requires that information should be given directly to the user and availability of the information somewhere is not enough.[166] In practice, however, users of cloud services are required to go through bulky privacy policies that are available online. For instance, a user of Google docs is

---

[159] Article 29 Working Party *Opinion 15/2011 on the definition of consent*, 2011 (WP187) p.17

[160] WP114 p.12

[161] WP187 p.19

[162] See (n 89)

[163] See in WP187 p.19

[164] Joint (2009) p.271

[165] WP187 p.20

[166] Ibid

required to go through Google's Universal Terms of Service, Additional Terms, Program Policies, Privacy Policy, and Copyright Notices.[167] This hardly enables the user to make an informed consent.

Further, consent must be freely given. This means the data subject must exercise free choice without any coercion, deception, or fear of negative consequences.[168] Thus, employers cannot rely on the consent of their employees for outsourcing processing as the nature of the relationship deprives the employee to choose freely due to fear of different treatment in case of refusal to consent. Besides, freely given consent implies a right to withdraw such consent once given.[169] The A29WP also opined that if no effective withdrawal is permitted, consent is considered to be deficient.[170] But there is an apparent incompliance by providers. A prominent example is Facebook where it is not possible to withdraw consent and stop further processing of your personal data. The only option Facebook allows you to do is to deactivate your account, not to delete it. Despite this, reinforcing the right to withdraw consent is paramount importance in the cloud as cloud users get concert experiences after using certain cloud service. Thus an express recognition of such right in the ongoing revision of the directive merits consideration.

Besides, Articles 7(a) and 26(1(a) require for the consent to be 'unambiguous'. Unambiguous consent requires that the indication signifying consent must not leave any doubt about the data subject's intent.[171] But it is hard to consider continuous use of a service that cloud providers infer consent from, to be doubt-free. 'Unambiguous' consent also excludes the inference of consent from inaction or silence of the data subject or cloud user.[172] Such an issue arises in relation to default privacy settings. For instance, in Facebook, the personal data of the user will be viewable by friends of

[167] Svantesson (2010a) p.396

[168] WP187 p.12

[169] Kuner (2007) p.212

[170] WP187 p.13

[171] WP187 p.21

[172] WP187 p.24

friends unless the user has changed the privacy setting.[173] Here the lack of action (failing to reset the default) is taken as consent by the user to make his data viewable by friends of friends. It is contentious to state that such consent is 'unambiguous'.

Worst the problem comes, same default setting is used with regard to religious and political views that are considered sensitive personal data pursuant to Article 8 that needs an 'explicit' consent which is higher in standard than 'unambiguous'. The term 'explicit' clearly is incompatible with opt-out solutions.

The above discussion unearths how the legitimacy of consent is challenged by the very nature of cloud and calls for consideration of the unique features of such technologies in providing legal basis for processing.

4.5 Jurisdiction and applicable law in cross-border clouds

4.5.1 Jurisdiction

The distinction between choice of law (choice of applicable law) and choice of jurisdiction (forum) provisions is far from being clear particularly in case of data protection laws.[174] A prominent example is found in Article 4 of the EUDPD. On the one hand, there are firm arguments that Article 4 should not be regarded as a jurisdiction provision as it would unnecessarily expand the basis for personal jurisdiction and thereby intrude with the notice, fairness, comity and national sovereignty principles.[175] The existence in the directive of rules specifically dealing with jurisdiction also counts in favor of this argument.[176] On the other side, there are arguments that Article 4 is not only a choice of law provision but also a basis for jurisdiction. Such seems the approach adopted by some DPAs[177] and A29WP[178].

---

[173] WP187 p.24

[174] Kuner (2010b) p. 176

[175] Swire (1998) p.1010

[176] Kuner (2007) p.112

[177] Ibid

[178] Kuner (2010b) p.7

Posit Article 4 is also jurisdiction clause, the argument that it unnecessarily expands basis for jurisdiction seems exaggerated. Bar Article 4(1(c)), the provision bases jurisdiction on the place of establishment of the data controller which is well accepted jurisdictional basis in different circumstances.[179] Even the basis in 4(1(c)) is not an entirely illegitimate as its base can be found in the objective territoriality, protective or effects doctrine of jurisdiction which are widely accepted bases,[180] albeit exorbitant. But such is not unfamiliar. For instance, US's general jurisdiction based on web-based stores in the online context is subject to same attack.[181] Even the claim that the existence in the directive of specific rules dealing with jurisdiction (Article 28(6)) not to regard Article 4 as jurisdiction clause is far from convincing. This arises as Article 28(6) deals with the allocation of jurisdiction among DPAs rather than International jurisdiction of courts.[182] Consequently it seems viable to argue that the arguments to exclude Article 4 form being regarded as jurisdiction clause are delicate.

On the other side, it has been claimed that even considering Article 4 only as applicable law provision, it can achieve same purpose as it is also a jurisdiction clause. This flows from the protective nature of data protection laws (that flows from its base in human rights) that "allows the assertion of regulatory authority over the data without having the entity processing the data be subject to the forum's power; i.e., forum law is applied to data processing for protective reasons as the next best thing to asserting jurisdiction."[183] Does this mean that it is irrelevant whether Article 4 is considered as only applicable law provision or also as jurisdiction provision?

Consideration of the implications of both scenarios is relevant here. Scenario 1: Article 4 is only choice of law provision. Commentators who argue in favor of this position claimed that Article 4 comes in to play when the usual jurisdictional principles point to

[179] Kuner (2010b) p.16

[180] Kuner (2010b) p.18-21

[181] Svantesson (2007) p.260

[182] Kuner (2010b) p.7

[183] Kuner (2010b) p.8

an EU member state.[184] One such law, at least in case of data protection claims of civil nature is the Brussels Regulation.[185] However, the application of the Brussels Regulation[186] is limited to cases where the defendant is established in an EU member state (Article 4(1)). Lacking an international instrument on the area, the jurisdictional rules of each nation comes in to play where the data controller is established outside EU and doesn't have an establishment for the purpose of the regulation (Article 4(1)). One such case is where a controller established outside-EU and doesn't have any establishment within EU '*makes use of equipment'* located in an EU member state.

In such situations where the applicable national choice of jurisdiction rules point to non-EU country, Article 4(1(c)) will not apply unless the equipment is considered as branch or establishment, which is another controversial matter.[187] Thus, scenario 1 opens a door for the evasion of EU law despite the fact that Article 4's main purpose is to avoid such specific circumvention possibilities as vociferously contemplated under Recital 20 of the directive.

This implies that providers who 'makes use of equipment' to transfer personal data outside EEA can escape application of EU law. However, some of the methods of transfer such as Safe Harbor, BCRs and Standard contractual clauses more or less address jurisdictional issues in advance. Furthermore, the usual connecting factors for jurisdiction fit uneasily to cross-border clouds. In case of tort the courts of the place where the harmful event occurs, in case of contract the courts of the place of performance are commonly used grounds in many jurisdictions. In a typical cloud scenario, where data are distributed in numerous servers across different jurisdictions, it is difficult to point to the place where damage occurred or the place where the contract is performed. This is because the damage that gives rise to liability can also be distributed in the same manner as the servers across different jurisdictions. Similarly, performance of contract can also be executed by providing computing power from

[184] Swire (1998) p.1013

[185] Kuner (2007) p.113

[186] Regulation No 44/2001/EC

[187] Swire (1998) p.1013

servers distributed across different jurisdictions. This unearths how these connecting factors are back-dropped in relation to new technologies, such as cloud computing.

Scenario 2: Article 4 is also a jurisdiction provision. The main concern with this scenario is its legitimacy, particularly in relation to Article 4(1(c)). Despite claims that Article 4(1(c)) is based on well accepted principles of jurisdictions, the resulting interpretation of the term 'makes use of equipment' to include personal computers, telecommunication networks, and cookies[188] will make it strikingly exorbitant under international law. Such wide interpretation which unnecessarily expands the jurisdiction goes beyond the very content of the article. The main advantage of scenario 2 is that it avoids the circumvention possibility in scenario 1 i.e. when the controller is established outside EU and 'makes use of the equipment'.

Nonetheless, the fact that the application of Article 4 (posit it is jurisdiction provision) will depend on identification of controller is problematic in cloud cases. This is because there are uncertainties regarding when exactly a party shall be considered as 'controller' in general and in the cloud in particular, if at all. Further, the controversies associated with 'makes use of equipment' discussed in section below is also relevant.

Thus, it seems appropriate, to argue that the safer approach is to consider Article 4 not only as applicable law provision but also as jurisdiction clause as it avoids the circumvention of the EU data protection law by merely relocating place of establishment outside EU, which is against the central aim of the directive. The fact that some DPAs also follow such a position could also further support such proposition. It also shows that such an approach can survive, at least as a short-term solution. However, it's being exorbitant, which in turn results in low chance of enforcement, can question its legitimate acceptance as a 'law' by controllers'.[189] Nonetheless, as long as a realistic interpretation to the phrase 'use of equipment' has been adopted, the concern can be mitigated. But such approach should be favored, awaiting better solution from

---

[188] *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites* , 2002 (WP56)

[189] Kuner (2010c) p.15

the legislator, as the best between the Scylla and Charybdis, as it prevents further threat to the rights of individuals.

4.5.2 Applicable law

Before beginning this discussion, it is worth noting the ambiguity that springs from the interaction between the direct applicability of EU law under Article 4, particularly sub-paragraph 1(c) and the need to provide legal basis under articles 25 and 26 of the directive. This is the case where a controller established for instance in the US and is member of Safe Harbor makes use of equipment (for instance cookies) located in one of the member states.[190] The question is whether such controller has to adhere to the full regime of the law of member state or to the principles of Safe Harbor or both. There are claims that such controller should have to comply with both the Safe Harbor principles and the applicable national law as determined by Article 4.[191]

Against this, it has been claimed that as far as the EU law is applicable pursuant to Article 4, there is no need to comply with the requirements of Articles 25 and 26.[192] There are also assertions, in such circumstance, that the controller should be subject to the full regime of the Directive and not to the more flexible regime of transfer of data to third countries.[193] Thus, the application of the stricter full regime under Article 4 swallows and renders it unnecessary to apply Articles 25 and 26. This seems to make sense as the rationale for regulating cross-border data flow is to avoid the circumvention of the application of substantive data protection principles than a substantive data protection principle in itself. Thus, as long as these principles are complied with, there is no need to resort to the cross-border regime. Nonetheless, the wide interpretation of 'makes use of equipment', it has been claimed, will render the provisions dealing with the transfer of data to third countries "superfluous as the directive would apply fully to

[190] Kuner (2007) p.167

[191] See citations in Kuner (2007) p.167

[192] Kuner (2007) p.167

[193] Terwangne (1997) p.238

every controller from the moment the information is collected over the Internet".[194] Such an approach, however, remains tenable as long as the global application of Article 4 can be diminished. One suggestion is to limit the application of Article 4(1(c)) to situations in which "data subjects are deprived by an artificial maneuver, of the benefit of the protection afforded by the Directive and situations which fall outside the scope of any protection whatsoever, even that concerning transborder data flows".[195] Despite such proposals, the interaction between the two remains far from clear.

With regard to application of Article 4, sub-paragraphs 1(a) and 1(c) are at focus, with sub-paragraph 1(b) left from discussion due to lesser practical significance. Article 4(1(a)) applies 'to processing of personal data in the context of an establishment of the controller on the territory of a member state'. This means the formal place of establishment as well as the place of actual processing is not relevant for the applicability of the directive if the processing is carried out in the context of the activities of an establishment of a controller which is located on community territory.[196] This is essential to cross-border cloud services as it would otherwise hinder its application due to the difficulty in locating where the processing is taking place across jurisdictions. The A29WP has opined that the notion of 'context of activities' requires determination of "who is doing what, whether an activity involves data processing or not, which processing is taking place in context of which activity".[197] Where the controller is established in several member states, it has to comply with laws of each member states. However, some DPAs, prominently Dutch, argue that Article 4(1(a)) adopts the country of origin principle and avoids the cumulative application of multiple laws.[198] Such an approach, however, is against the central objective of Article 4 as the

[194] Bergkamp (2000) p.100

[195] Terwangne (1997) p.238

[196] Moerel (2011a) p.29

[197] Article 29 Working Party *Opinion 8/2010 on applicable law*, 2010 (WP179) p.13

[198] Moerel (2011b) p.103

controller can avoid the applicability of the EU law by relocating its main establishment outside EEA.[199]

Two cross-border cloud computing scenarios will be considered here. Scenario 1: the user of cloud service is controller established in EU member state while the provider is a processor established and processing the data outside EEA. In this scenario the provider is processing on behalf of the EU controller and such processing is considered in the context the activities of the establishment in the Community. This results in the application of EUDPD to the processing in third country.[200] Nonetheless, multinational companies with subsidiaries in different member states which adopted such cloud service are required to comply with the laws of all member states where these subsidiaries are situated as long as the processing takes place in the context of the activities of these establishments. With the existing variations in implementing the cross-border provisions of the directive among member states,[201] multinational companies are deprived of the benefit to outsource processing under the same condition which in turn can disadvantage business.

Scenario 2, essentially the same as scenario 1 but the cloud provider is a controller. This is the case where the provider offers value added services by processing the personal data. In scenario 2 the provider, besides processing on behalf of the EU controller, also processes for purposes determined by him/jointly with the controller. Accordingly the discussion in the first scenario is relevant with regard to the processing by provider on behalf of the EU controller. But the question is if the processing by the provider (for the provision of the value added service) is subject to EU law pursuant to Article 4(1(a). Such determination hinges on whether the EU cloud user can be designated as establishment of the cloud provider and whether the processing, as determined by the provider is carried out in the context of the EU cloud user. Such assessment depends, according to ECJ's requirement for 'independent agent', on whether the third party is

[199] Moerel (2011b) p.96

[200] Moerel (2011a) p.30

[201] Kuner (2007) p.162

under the direction and control of the controller.[202] This equally applies, to a possible scenario 3, where controller from outside EEA outsources the processing to cloud provider within the community. But it is less likely that such third parties would qualify as establishment under normal circumstance. Even if under exceptional circumstances it qualifies as establishment, it is less likely that the processing is carried out 'in the context of the EU cloud user' as it is the provider that determines the purpose and means. But such situation could be different when the cloud user is considered joint controller with the provider for the processing due to its involvement in determining the means and purpose. Consequently, Articles 4(1(a)) will not normally apply to scenarios 2 and 3. But they can still fall under Article 4(1(c)).

No provision of the directive has caused more controversy than of Article 4(1(c)).[203] The provision designates the law of a member state to apply when 'the controller is not established on community territory and for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of member state, unless such equipment is used only for purposes of transit..' The controversy over the provision is exacerbated by the expansive interpretation given to the term 'makes use of equipment' by the A29WP to encompass personal computers, cookies or JavaScript besides surveys, questionnaires and database.[204]

Here consideration will be given to Scenarios 2 and 3. However, scenario 1 is already a matter for Article 4(1(a)), as discussed above. With regard to the second scenario where both the EU user and the provider outside EU are controllers, if the cloud provider uses 'means 'or 'equipment' located in EU, it will be subject to the EUDPD.[205] Considering users' computer as equipment for the purpose of Article 4(1(c)) is highly disputed for it is interpreted that the computer is under the control of the user than the provider.[206]

---

[202] Moerel (2011a) p.35

[203] Kuner (2007) p.118

[204] WP179

[205] See example 8 WP179

[206] See Kuner (2007) p.120 and Moerel (2011a) p.38

Despite same argument with regard to cookies as they can be disabled by the user,[207] there seems a slight consensus to qualify as 'make use of equipment' at least when they are used in a non-transparent way.[208] Thus the fact that many cloud providers, particularly those offering consumer clouds, uses cookies will render them subject to EU data protection law.

With regard to scenario 3 where a controller from outside EU outsources to cloud provider in the community territory, the A29WP has clearly pointed out that such processing will be subject to EU law pursuant to Article 4(1(c)) provided the processing is not carried in the context of activities of an establishment of the controller in EEA.[209] This is on consideration that the database and equipments to process the data are located in the EU qualifies for 'makes use of equipment'. This perhaps can imply that the controller has to justify under Articles 25 or 26, the re-exportation back of the data from the EEA. But if the above assertion, namely that the application of Article 4 excludes Articles 25 and 26, is upheld, it will avoid such an undesirable result. Such an approach has profound economic impact on EU cloud providers as it discourages controller outside EU to use cloud services within the community to escape the burdensome obligations in the directive. This is also acknowledged by the A29WP.[210] Salt in to the wound, the A29WP has exacerbated such a problem by extending the application of EU law in such cases also to the part of processing taking place in a third country.[211]

Besides, an intra-EU conflict of laws may arise due to the distribution of the equipment used across the member states. Further, the need to designate an actor as controller or processor both under Article 4(1(a) and 4(1(c)) fits uneasily in to the cloud, particularly cross-border ones, due to the involvement of myriad of actors with unclear roles and due to the difficulty to designate an actor as controller or processor.

---

[207] Moerel (2011a) p.39

[208] See Kuner (2007) p.127

[209] WP179 p.20

[210] WP179 p.24

[211] Ibid

Thus, we have noted above that there are spacious possibilities that cross-border cloud services can be subject to either Article 4(1(a)) or 4(1(c)) in which case the application of Articles 25 and 26 is deemed unnecessary if a restricted approach towards Article 4 is adopted.

4.6 Data Security in the cloud

Data security is at the fore of privacy concerns in the cloud. The physical impediments to security threat in the traditional IT model are vanished with the surfacing of cloud and anyone connected to the Internet can be a threat to security measure deployed anywhere. Such concern however mainly goes to public clouds due to their multi-tenancy nature as opposed to private clouds.

In the cloud, security threats can emanate from the cloud users themselves as cloud computing opens the possibility for spying and interfering in each other's activities, particularly among commercial rivalries.[212] It can also emanate from third party insiders (such as the provider's employees' and sub-contractors) in performing their functions for providing the service. Such can result in abuse or sabotage of the data for purposes other than originally processed. In addition the cloud has taken the data closer to attacks by third party outsiders (with no connection to the provider) as the only barrier between data in the cloud and any person connected to the Internet remains simple password and username.[213] Of particular importance to cross-border cloud is also the possibility of access by law enforcement authorities when the processing is taking place in third countries.

The threats to security are amplified by the use of cloud computing power to facilitate the attack on security firewalls. Spammers have already purchased cloud services directly and launched phishing campaigns and hackers are making use of the availability of cryptographic key cracking cloud services.[214] This, together with the obscurity of identifying the actors responsible after security breach has occurred led

[212] Mowbray (2009) p.143

[213] Joint (2009) p.271

[214] Jansen (2011) p.12

people to question if it would ever be possible to ensure security in the cloud.[215] The paragraphs below will substantiate such a quest in light of the security measures in the EUDPD.

Article 17(1) of EUDPD requires controllers to '*implement appropriate technical and organizational measures to protect personal data …'* Where processing is to be carried out by third party on behalf of the controller, the later must choose a processor having the appropriate technical and organizational measures in place and that ensures its compliance (Article 17(2)). This can be done by contract or another binding act (Article 17(3)).

Nonetheless the fact that the cloud obscures the location and jurisdiction of the data processing means it is difficult for controllers situated in Europe to effectively ascertain whether such measures are in place. The involvement of sub-processors, mostly without the knowledge of the controller makes it more difficult even to effectively fathom who and where the processing is taking place. Despite possibilities for contractual measures, it seems providers are not ready to commit to security requirements of users' preferring to implement widely recognized technical standards, if at all.[216] Where they did, its enforceability in time of failure seems far from being easy when the provider doesn't have any assets in the EEA.

Furthermore, Article 28(3) reinforces Article 17 by giving DPAs the power to check whether the controller has put in place the necessary technical and organizational measures and take appropriate action. But this seems non-existent in case of cross-border clouds where EU DPAs lacks the sovereign power to check whether provider in third country has already put such measures in place. Even within EEA where such monitoring is theoretically possible, there is no actual implementation of it.[217]

Third party access is at the gist of the concerns in cross-border cloud services. Third party litigants can easily get records from the cloud provider as the later has less

---

[215] Dhillon (2011) p.346

[216] Balboni (2010) p.8

[217] Weichert (2011) p.8

motivation to resist handing over compared to the user particularly in those countries with no privacy legislation.[218] Government authorities such as Police, national secret services, and financial authorities can have statutory authority to access data of cloud users not only for 'public security' reasons but also for economic espionage in the domestic interest.[219] Such threat is more perilous when the third country is undemocratic that doesn't respect human rights and International treaties and persecuting targeted individuals on political, ethnic, religious and other grounds.[220] But even Western Democracies have laws allowing government authorities to access records with prominent examples the USA PATRIOT Act 2001and UK Regulation of Investigatory Powers Act 2000 that allows for access of electronic documents.[221] Notwithstanding this, when they think it is important for national interest, governments does not necessarily need a law authorizing such access. [222]

IP law, law of confidence and perhaps unlawful enrichment could mitigate an economic loss due to the user as a result of the data falling in to the hands of third party because of security breakdown. But the territorial limitation of such laws holds them short of having any help to the user in case of cross-border clouds. After all such assertion is plausible only when possible to point towards whose hands the data falls, which is not easy in cloud cases in general.

Data zoning (processing data from EU within EU) has emerged as a response to the threats of third party access. But such an undertaking doesn't necessarily guarantee the above threat is averted. Firstly, providers' are silent with the location of cloud generated data which could cause no lesser threat if accessed. Secondly, there are claims that such commitments do not exclude replication of the data outside the claimed data zone and questions also arise as to their reliability.[223] Thirdly, as long as the providers' are

---

[218] Gellman (2009) p.14

[219] Weichert (2011) p.7

[220] Ibid

[221] Mowbray (2009) p.135

[222] Mowbray (2009) p.135

[223] Hon (2011c) p.8

subject to the laws of certain jurisdiction, access to the relevant authorities can be granted remotely if necessary.[224] This is particularly the case when there are no sufficient measures in place.

Ways forward:

Technical measures such as anonymization and pseudonymization are promoted to alleviate such concerns. Despite mitigating the risk of identification their significance is being questioned with the advancement of de-anonymization technology and ubiquity of information in the Internet.[225] Consequently there are claims that practices of selling anonymized or pseudonymized personal data of users should be revisited.[226] The uncertainty within EU regarding the treatment of such data also affects their wider usage in the region. Another technical measure of paramount importance is encryption. Encryption can be deployed to protect data in transit, rest or in processing. Nonetheless, the state of the art has yet to develop for encryption in case of processing. There are some claims, however, that homomorphic encryption enables SaaS providers to process while encrypted and providers and governments will not be able to decrypt such kind of data.[227] But its relevance is limited only to simple arithmetic calculations.[228]

Effective encryption can lower the above threats but it is not panacea. Mostly government authorities get sufficient resources to decrypt an encrypted data and force parties into handing over decryption keys backed by statutory restrictions on use of certain encryption methods. Absent this, they can still force providers to add a backdoor that would steal the users' key. [229] However, the above technical measures remain vital as they mitigate the risks associated. They also remain vital because they increase the cost of identification.[230] A combination of anonymization/pseudonymization then

---

[224] Hon (2011c) p.27

[225] Mowbray (2009) p.145

[226] Ibid

[227] Ruiter (2011) p.369

[228] Pieters (2011) p.449

[229] Soghoian (2010) p.420

[230] Soghoian (2010) p.398

decryption can take security one step ahead and should be promoted. Fragmented storage of data across jurisdictions can also be of particular importance for such threats.

Sometimes providers already put these technical measures in place. For instance Google offers HTTPS encryption for its Docs, Spreadsheets, and Calendar services, but is not turned on by default.[231] But the users lack the vim to turn on such settings for, *interalia*, awareness reasons as to the consequences thereof.[232] Awareness raising mechanisms for users as to the virtues of such technical measures should also be considered. Imposing an obligation on providers to notify users the risks of using clouds without these technical measures in place is one way of raising such awareness.[233]

Increasing users control over data and transparency of providers towards users with regard to the appropriate technical and organizational measures have also been promoted as way forward. Particularly, Open-Software framework that allows users to run and control entire virtual machine instance across physical devices have been recommended.[234] But such can be risky for average users with scarce security awareness unless backed by providers' robust security protection measures. It still remains vital as an additional layer to the above measures.

Recent treatise has emphasized the value of human actors.[235] It has been claimed that the role of human actors, business structures and processes have been overlooked or inadequately addressed and thus calling for issues such as responsibility, integrity of individuals, trust and ethics to be addressed.[236] It is a call for *Socio-Technical* approach in managing information security in the cloud.[237] Despite this, technical measures should remain at the forefront and should not be displaced by social factors.

---

[231] Soghoian (2010) p.381

[232] Soghoian (2010) p.382

[233] Ibid

[234] Dhillon (2011) p.351

[235] Dhillon (2011) and Pieters (2011)

[236] Dhillon (2011) p.356

[237] Ibid

Finally, albeit very importantly, the onus remains on the legislator to weigh the above policy considerations and translate them in to binding and enforceable rights and obligations of the parties involved.

4.7 Implications of the ECJ's Decision on *Bodil Lindqvist*[238]

The *Lindqvist* decision was the first ruling of the ECJ where the application to the Internet of the provisions on International transfer was tested. Despite that it is criticized for offering less delineation and clarity than observers hoped.[239] In that case Swedish woman –Bodil Lindqvist- who uploaded personal data of her colleagues without their permission into an Internet page she created, was punished for transferring data to third country by making it accessible to Internet users outside EEA.[240] Upon appeal, a reference was made for the guidance of the ECJ.[241] One of the questions referred, which is relevant here was:

If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden - with the result that personal data become accessible to people in third countries - does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?[242]

The ECJ response to the question was it doesn't constitute transfer to third country because there were no direct transfer between the person who accessed the data from third country and the person uploading the data but through the computer infrastructure of the hosting provider where the page is stored. [243] The Court added that considering the state of development of the Internet at the time the directive was drawn up, it

---

[238] Case C-101/01 [2003] ECR I-12971

[239] Garcia (2005) p.1207

[240] Case C-101/01 Parg12-14 and 16-18

[241] Case C-101/01 Parg16-18

[242] Case C-101/01 Parg18

[243] Case C-101/01 Parg60-61

doesn't seem to be the intention of the legislator to encompass circumstances such as *Lindqvist's* case within the expression 'transfer'.[244] Further, the Court has noted that if every time personal data are loaded to the Internet is considered as a transfer to third country, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the Internet.[245] The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the Internet.[246] Finally considering that operations such as those carried out by *Lindqvist* do not as such constitute a transfer of data to third country, the Court found it unnecessary to investigate whether an individual from third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country.[247]

Implications to cross-border cloud Services:

It has been claimed that the *Lindqvist* decision suggests if cloud user uploads personal data to data centers of a provider established within the EEA it wouldn't constitute transfer to third country irrespective of the location of the data centers.[248] But the validity of such an interpretation is questionable. This is because, it has been argued that the *Lindqvist* decision seems to suggest "while it may be difficult to argue that her conduct didn't amount to a transfer, the consequence of reaching such a finding would be devastating for the technology in question- a reasonableness test was applied".[249] A contrario reading of this means even acts such as of *Lindqvist* involves transfer of data and could have been considered as transfer to third country if not for the devastating consequence to the technology. Making the provisions of chapter IV of the directive of general application to the Internet as such was the devastating consequence recognized

[244] Case C-101/01 Parg68

[245] Case C-101/01 Parg69

[246] Case C-101/01 Parg69

[247] Case C-101/01 Parg70

[248] Hon (2011c) p.9

[249] Svantesson (2010b) p.15

in *Lindqvist*.[250] This implies, in case of acts such of *Lindqvist*, whether a transfer to third country exists or not hinges on assessment of the consequences if considered transfer, not on where the provider is established. It is not assumed that all situations of cross-border clouds will result in such devastating consequence. One such situation is where business cloud users upload personal data in to servers of provider located outside EEA to be accessed only by them or their subsidiaries. In such a case there is no risk that the provisions in chapter IV will become of general application to the Internet.

Further, the above[251] interpretation fails to appreciate the risks associated when data is located outside EEA regardless of where the provider is established unless necessary technical measures are in place. The fact that a provider is established within EEA doesn't guarantee that the risks where the provisions on transfer are meant to avoid are averted. A prominent example is the SWIFT case where a Belgian established financial institution gave access to US authorities to the data which is mirrored for backup reasons from its servers located in EU territory to its servers in the US.[252] Such risks are more serious when the servers are operated by third party such as in typical cloud because of risk of additional accesses by third parties connected with the provider. This has led the A29WP to consider SWIFT's act as a transfer to third country even though it is established in Belgium.[253] But it should also be noted that data is in servers located within EEA doesn't guarantee that it is all secure as access can be granted remotely to third parties unless the appropriate technical measures are in place as in the discussion below.

On the other hand it has been alleged that, considering the fact specific nature of the case, the *Lindqvist* judgment doesn't suggest granting of access is not a 'transfer' in all circumstances.[254] Granting access of personal data by making it available in the Internet

---

[250] Case C-101/01 Parg69

[251] (n 248)

[252] Article 29 Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT),* 2006 (*WP128)* p.2

[253] WP128 p.21

[254] Kuner (2007) p.82

on large scale and for business purposes could qualify as transfer in the Directive.[255] Translated to cloud situations, this means even uploading a data in to servers within EEA could qualify as transfer to third country if access has been granted to third parties outside EEA to the data within these servers provided it is on large scale and for business purposes. Uploading personal data in large scale and for business purposes in to provider's servers located outside EEA and granting access to third parties of such data would, *a fortiori*, constitute transfer to third country. Terminologically, is accessing data remotely from servers within EU qualifies as 'transfer to third country' remains questionable. Furthermore it would also be difficult to prove whether access has been granted to third party or not in cloud cases. But that remains logical as far as the risk to such data is not different from other cases of transfer. The 'large scale and business purpose' requirement seems to exclude the situation where individuals upload personal data of friends in to social networking sites. But is it necessary that an access should be granted and such access should be 'on large scale and for business purpose' even where the data is uploaded to servers located outside EEA?

In this regard it has been asserted that the court's finding in *Lindqvist* was on the basis that transfer only exists when personal data are actually received in third country; not when data is available on the Internet and could have been received.[256] This implies if uploading the data in to servers of the provider located outside EU is considered as 'received' by the servers in that country, it involves a transfer to third country irrespective of it is in large scale and for business purposes. The author believes such should be the case. But if 'reception' requires some human element (such as access by third party) as in the above case where the servers are within EEA, it would not constitute transfer to third country. But the author believes that actual access should not be a requirement at least where the servers are located outside EEA. Firstly, it is difficult to prove. Secondly, even the directive's general approach on international transfers is not based on actual violation of data protection principles, rather based on the assumption that risk of non-compliance is higher in those countries with no

[255] Kuner (2007) p.156

[256] Ibid

adequate protection than in those that ensure adequate protection. Thus, the determining factor should be whether there is risk (of access) taking all the technical and organizational measures in place.

Posit the 'large scale and for business purpose' requirement doesn't apply in case the servers of the provider are located outside EEA; the foreseeable problem is that individual cloud users can be subject to the provisions of chapter IV. Such results in enforceability problem that the ECJ wishes to avoid. But there are claims that the practical problems in subjecting individuals to regulatory regime do not differ from those that that are topical within other fields of data protection.[257] At the same time such problem shouldn't be overlooked either. Thus, it is for the legislator to find the right balance.

Therefore, the safer way of implicating the *Lindqvist* judgment to the cross-border clouds should accordingly be that the assessment of whether there is transfer to third country shouldn't hinge on either location of the data or establishment of the provider. It should rather be based on the potential and actual risks (of access) that exist considering the circumstance of each case, particularly the appropriate technical and organizational measures in place.

[257] Blume (2004) p.305

5 Conclusion

Despite its significant business benefits, cloud computing has posed a regulatory challenge on the application of data protection rules. Of particular challenge is to the regime regulating cross-border data flow as the cloud has obscured the concepts of data location and a particular receiver or destination that are basic for such regimes. In this thesis I considered the challenges in light of the European directive. It has been shown that the cloud has blurred the distinction between the concepts of controller and processor maintained in the directive. Further, it has brought new privacy concerns such as lock-in and enlarged some of the existing ones (e.g. profiling and information ownership issues). I have also maintained that the adequacy approach of the directive that requires ascertaining the location and the receiver of the data is in clear contradiction with the very nature of the cloud and the Internet in general.

The directive's assumption that data transferred outside EEA is under more security threat than data that remained in the community is no longer viable. It is susceptible to circumvention by granting remote access. Equally the same threat can subsist over data within the community as far as all necessary technical and organizational measures are not taken. Similarly a data can remain secure regardless of its location if all the appropriate technical and organizational measures are in place. Thus, a shift from location of data as criteria seems inevitable perhaps to risk (of access by unauthorized parties) taking account of all the security measures in place. An introduction of the 'more or less' protection of personal data could also merit consideration.

Further, it has been demonstrated that the legal grounds in the directive to transfer data outside EEA fits uneasily in to the cloud. There are difficulties in using the standard contractual clauses, BCRs and Safe Harbor to transfer data in to cloud. The cloud has made it strikingly difficult to use consent as a legal base for the transfer due to the difficulty in depicting the circumstances necessary in obtaining valid consent.

It has also been noted that there is some truth in the assertion that the use of Article 4 of

the directive as choice of forum provision unnecessarily expands claim for personal jurisdiction albeit exaggerated. It is the interpretations rather than the very content that results in such an undesirable end. But most of the connecting factors in Article 4 are based on well accepted principles. Thus, awaiting better solution, the use of Article 4 (also as a choice of forum provision) is recommended as it avoids a possible legal loophole where EU law might not be applicable.

Additionally, it has also been shown that Article 4 applies to many cross-border cloud situations. This occurs when controllers established in the EEA outsource processing to providers outside EEA and that processing is taking place in the 'context of the activities' the controller within the EEA (Article 4(1(a)) or when providers established outside EEA processes data of EU citizens using an equipment/means located within EEA or when controllers established outside EEA uses data centers located within EEA (4(1(c)). Particular attention is required towards the application of EU law when controllers from outside EEA uses data centers located in EU. This can have serious economic impact on cloud providers inside the community, especially if the re-exportation back of such data needs compliance with the data transfer restrictions. However maintaining that, it has been suggested, the restrictions on data transfer will not apply in case Article 4 applies can avoid such concern albeit with enforcement unease.

Furthermore, the wider usage of cloud computing has been challenged by the security concerns associated with it. Security threats can emanate from the users themselves, from third party insiders and third party outsiders. Of particular importance to cross-border clouds is access by government authorities in the third country. Technical measures such as anonymization/pseudonymzation and encryption has proven sufficient at least in mitigating the associated risks, though they are not panacea. Combination of anonymization/pseudonymization or/and data fragmentation followed by encryption can justify promoting. User awareness raising and promoting transparency within providers can enhance the effectiveness of such measures. Finally focus on the human factor is also firmly promoted by some authors. Though commendable, its particular importance to the cloud and cross-border clouds in particular might warrant further research.

With the computer technology and IT continuing to progress at an astounding rate, so does cloud computing. This will offer users significantly lower priced services with very attractive features than before. It is my opinion that with such development more data is expected to migrate to the cloud. Against this, the hurdles in adopting cloud services are likely to diminish over time. With a foreseeable development of Industry standards and code of practices,[258] concerns over compatibility, lock-in and reliability are expected to ebb. A parallel development in security technologies will resolve the associated security concerns. Moreover, when laws are tailored to accommodate cloud architecture, cloud will continue to become more and more compliant to the legal requirements. The ongoing review of the EUDPD is an exemplary move to tailor laws to fit the cloud.

[258] See Marchini (2010) p.150 on the initiatives from the cloud industry in developing codes of practice and standards with regard to issues of transparency, information security and data protection

Reference table

Legislations

EU Instruments

Council Regulation (EC) 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177

Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 012, 16/01/2001, pp. 0001 – 0023.

Council Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17/07/2000, pp. 0001 – 0016.

Council Directive 96/9/EC of 11 March on the legal protection of databases [1996] L77

Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to processing of personal data and the free movement of such data [1995] OJ L281

Council Directive 93/13/EEC of April 5 1993 on unfair terms in consumer contracts [1993] OJ L095

Other Instruments

Australian Privacy Act 2001 available:

http://www.privacy.gov.au/materials/types/infosheets/view/6583

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act 2001

UK Unfair Contracts Act 1977 available: http://www.legislation.gov.uk/ukpga/1977/50/pdfs/ukpga_19770050_en.pdf

UK Regulation of Investigatory Powers Act 2000 available: http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

Cases

ECJ Judgment in Bodil Lindqvist Case C-101/01 [2003] ECR I-12971

British Horseracing Board v. William Hill Organization (Case C-203/02) [2005] ECDR 1

Article 29 Working Documents

Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent* adopted on 13 July 2011 (WP187)

Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor'* adopted on 16 February 2010 (WP169)

Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law* adopted on 16 December 2010 (WP179)

Article 29 Data Protection Working Party *Opinion 4/2007 on the concept of personal data* adopted 20 June 2007 (WP136)

Article 29 Data Protection Working Party *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* adopted on 22 November 2006 (WP128)

Working document on a common interpretation of Article 26(1) of Directive 95/46/EC

adopted on 25 November 2005 (WP114)

Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites adopted on 30 May 2002 (WP56)

Secondary Literatures

Books

Bygrave Lee, *Data Protection Law: Approaching Its Rationale, Logic and Limit.* The Hague, (Kluwer Law International) 2002

Kuner Christopher, *European Data Protection Law: Corporate Compliance and Regulation* (2nd Ed.) New York, (Oxford University Press) 2007

Lessing, Lawrence, *CODE 2.0*. New York, (Basic Books) 2006

Marchini Renzo, *Cloud Computing: A practical Introduction to the Legal Issues*. London (British Standards Institution) 2010

Svantesson Dan B, *Private International Law and the Internet.* The Hague, (Kluwer Law International) 2007

Computers, Privacy and Data protection: an element of Choice. Serge Gutwirth …[et al] (eds.) London, New York, *(*Springer) 2011

Reinventing Data Protection. Serge Gutwirth … [et al] (eds.) London, (Springer) 2009

Proceedings of the 2009 ACM workshop on Cloud computing security. Radu Sion and Dawn Song (chairs). Chicago, Illinois (ACM) 2009 <http://dl.acm.org/citation.cfm?id=1655008> accessed 3 September 2011

The Data Protection Directive and Medical Research Across Europe. Deryck Beyleveld… [et al] (eds.) Burlington, (Ashgate Publishing Ltd) 2004

Articles

Balboni Paolo. *Data Protection and Data Security Issues Related to Cloud Computing in the EU*. (2010) Tilburg University Legal Studies Working Paper Series No. 022/2010, <http://ssrn.com/abstract=1661437> accessed 20 September 2011

Bergkamp L and J Dhont. *Data Protection and the Internet: An analysis of the European Community's Privacy Legislation in the Context of World Wide Web*. In: EDI Law Review (2000)

Blume Peter. *Data Protection in the Private Sector*. In: Scandinavian Studies in Law. Vol.47 (2004)

Bradshaw Simon, Christopher Millard and Ian Walden. *Contract for clouds: comparison and analysis of the terms and conditions of cloud computing services.* (September 2, 2010) Queen Marry School of Law Legal Studies Research Paper No.63/2010, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id¼1662374> accessed 15 August 2011

Bygrave Lee. *Privacy and Data Protection in an International Perspective*. In: Scandinavian Studies in Law. Vol 56 (2010)

Casabona Carlos M.R. *Anonymization and Pseudonymization: The legal framework at European Level*. In: Deryck Beyleveld and others (eds.) The Data Protection Directive and Medical Research Across Europe. Burlington, (Ashgate Publishing Ltd) 2004. Pp.33-49

Comment. *Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and their Successors*. In: San Diego Law Review. Vol. 34 (1997)

Chow Richard… [et al]. *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control.* In: Radu Sion and Dawn Song (chairs), Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, Illinois, (ACM) 2009. Pp.85-90

Catteddu Daniele and Giles Hogben. *Cloud Computing - Benefits, risks and*

*recommendations for information security. (*European Network and information Security Agency 2009)

Dhillon Gurpreet and Ella Kolkowska. *Can a Cloud Be Really Secure? A Socratic Dialogue.* In: Serge Gutwirth… [et al] (eds.) Computers, Privacy and Data protection: an element of Choice. London, New York, (Springer) 2011. Pp.345-360

Garcia F. J. *Bodil Lidnqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators*. In: Fordham Intellectual Property, Media & Entertainment Law Journal. Vol. XV (2005)

Gavison R. *Privacy and the Limits of Law.* In: The Yale Law Journal. Vol.89 (1980)

Gellman Robert. *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing.* (World Privacy Forum February 23, 2009)

Hildebrandt Mireille. *Who is profiling who? Invisible Visibility.* In: Serge Gutwirth… [et al] (eds.) Reinventing Data Protection? London, New York, (Springer) 2009. Pp.239-252

Hon (2011a) W Kuan, Christopher Millard and Ian Walden. *The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1*' (March 10, 2011) Queen Marry School of Law Legal Studies Research Paper No. 75/2011, <http://ssrn.com/abstract=1783577 accessed 5 August 2011

Hon (2011b) W Kuan, Christopher Millard and Ian Walden. *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2* (March 21, 2011) Queen Mary School of Law Legal Studies Research Paper No. 77/2011<http://ssrn.com/abstract=1794130 accessed 3 August 2011

Hon (2011c) W Kuan and Christopher Millard. *Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4* (October 28, 2011) Queen Mary School of Law Legal Studies Research Paper No. 85/2011. http://ssrn.com/abstract=1925066 accessed 30 October 2011

Jadhwanl Prem, John Mackinnon and Mohamed Elrefal. *Cloud Computing Building a*

Framework for Successful Transition. (2009) GTSI white paper, <http://www.gtsi.com/cms/documents/White-Papers/Cloud-Computing.pdf> accessed 6 August 2011

Jansen Wayne and Timothy Grance. *Guidelines on Security and Privacy in Public Cloud Computing* (National Institute of Standards and Technology 2011)

Jefery Keith and Burkhard Neidecker-Lutz. *THE FUTURE OF CLOUD COMPUTING OPPORTUNITIES FOR EUROPEAN CLOUD COMPUTING BEYOND 2010*. (Report presented to European Commission, Information Society & Media Directorate-General, 2010) <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf> accessed 18 November 2011

Joint Andrew… [et al]. *Hey, you, get off of that cloud*? In: Computer L & Security Rev. Vol.25 (2009)

Kroes Neelie. *Cloud computing and data protection.* (Les Assises du Numérique conference, Université Paris Dauphine, 25 November 2010) SPEECH/10/686

Kuner (2010a) Christopher. *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future*. (2010) TILT Law & Technology Working Paper No. 016/2010, < http://ssrn.com/abstract=1689483v> accessed 25 August 2011

Kuner (2010b) Christopher. *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)*. In: International Journal of Law and Information Technology. Vol.18 (2010), < http://ssrn.com/abstract=1496847> accessed 20 September 2011

Kuner (2010c) Christopher. *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2)*. In: International Journal of Law and Information Technology. Vol.18 (2010), <http://ssrn.com/abstract=1689495> accessed 20 September 2011

Kuner Christopher. *Developing an adequate legal framework for international data*

transfers. In Serge Gutwirth… [et al] (eds.). Reinventing Data Protection? London, New York, (Springer) 2009. Pp.263-273

Kuner Christopher. *Legal Aspects of Encryption on the Internet.* In: International Business Lawyer. Vol.24 (1996)

Meil P. and T.Grance. *The NIST Definition of Cloud Computing, Version 15.* (US National Institute of Standards and Technology 2009), <http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf> accessed 8 August 2011

Microsoft Corporation, *The economics of Clouds*. (2010), <http://www.microsoft.com/presspass/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf> accessed 11 August 2011

Moerel (2011a) Lokke. *The Long arm of EU data protection Law: Does the Data protection directive apply to processing of personal data of EU citizens by websites worldwide?* In: International Data Privacy Law. Vol.1.No.1. (2011)

Moerel (2011b) Lokke. *Back to Basics: when does EU data protection law apply?* In: International Data Privacy Law. Vol1.No.2. (2011)

Mowbray. *The Fog over the Grimpen Mire: Cloud Computing and the Law*. In: SCRIPTed. Vol.6.No.1. (2009)

OECD. *REPORT ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS*. (2006) OECD/OCDE, <www.oecd.org/sti/security-privacy> accessed 20 August 2011

Ohm Paul. *Broken Promises of Privacy: responding to the surprising failure of anonymization.* In UCLA Review. Vol.57. (2009) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006> accessed 30 August 2011

Perkins Aaron. *Encryption Use: Law and Anarchy on the Digital Frontier [comments]*. In: Houston Law Review. Vol.41.No.5. (2005)

Pew Internet & American Life Project. *Consumer Protection in Cloud Computing Services* (White paper on Best Practices From a Consumer Federation of America 2010)17 <http://whitepapers.zdnet.com/abstract.aspx?docid=2385447> accessed 15 September 2011

Pieters Wolter. *Security and Privacy in the Clouds: A Bird's Eye View.* In: Serge Gutwirth… [et al] (eds.) Computers, Privacy and Data Protection: an Element of Choice. London, New York, (Springer) 2011. Pp.445-457

Poullet Yves… [et al]. *Data protection in the clouds.* In: Serge Gutwirth… [et al] (eds.) Computers, Privacy and Data protection: an element of Choice. London, New York (Springer) 2011. Pp.377-409

Reed Chris. *Information 'Ownership' in the Cloud*. (March 2, 2010) Queen Mary University of London Legal Studies Research Paper No. 45/2010, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461> accessed 10 August 2011

Reding Viviane. *The upcoming data protection reform for the European Union*. In: International Data Privacy Law. Vol.1.No.1. (2011)

Robinson Neil… [et al]. *Review of the European Data Protection Directive*. (2009) RAND Europe technical report, <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf> accessed 28 August 2011

Ruiter Joep and Martijn Warnier. *Privacy Regulation for Cloud Computing: Compliance and Implementation in Theory and Practice.* In: Serge Gutwirth… [et al] (eds.) Computers, Privacy and Data protection: an element of Choice. London, New York, (Springer) 2011. Pp.361-376

Soghoian Christopher. *Caught In The Cloud: Privacy, Encryption, and Government Back Doors in the WEB 2.0 Era*. In: Telecomm. & High Tech. L.J. Vol.8. (2010)

Svantesson (2010a) Dan, Roger Clarke. *Privacy and consumer risks in cloud*

computing. In: Computer L and Security Rev. Vol.26. (2010)

Svantesson (2010b) D. *Privacy, Internet and Transborder Data Flows.* In: Masaryk University Journal of Law and Technology. Vol.4.No.1. (2010)

Swire Peter. *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*. In: International Lawyer. Vol.32. (1998)

Terwangne and Louveaux. *Data Protection and Online Networks*. In: Computer Law and Security Report. Vol. 13 No.4. (1997)

Walden I. *Anonymizing Personal Data.* In: International Journal of Law and Information Technology. Vol.10.No.2. (2002)

Wallis Paul. *A Brief History of Cloud Computing: Is the Cloud There Yet?* (SYS-CON Media, Inc. publication, 2008) <http://cloudcomputing.sys-con.com/node/581838#related> accessed 18 November 2011

Weichert Thilo. *Cloud Computing and Data Privacy*. (The Sedona Conference 2011)

A