Privacy Regulations for Cloud Computing

Compliance and Implementation in Theory and Practice

Joep Ruiter
Faculty of Sciences, VU University Amsterdam
jrr260@few.vu.nl

Martijn Warnier
Faculty of Technology, Policy and Management,
Delft University of Technology
M.E.Warnier@tudelft.nl

1 Introduction

Privacy is considered to be a fundamental human right (Movius and Krup, 2009). Around the world this has led to a large amount of legislation in the area of privacy. Nearly all national governments have imposed local privacy legislation. In the United States several states have imposed their own privacy legislation. In order to maintain a manageable scope this paper only addresses European Union wide and federal United States laws. In addition several US industry (self) regulations are also considered.

Privacy regulations in emerging technologies are surrounded by uncertainty. This paper aims to clarify the uncertainty relating to privacy regulations with respect to Cloud Computing[1] and to identify the main open issues that need to be addressed for further research. This paper is based on existing literature and a series of interviews and questionnaires with various Cloud Service Providers (CSPs) that have been performed for the first author's MSc thesis (Ruiter, 2009). The interviews and questionnaires resulted in data on privacy and security procedures from ten CSPs and while this number is by no means large enough to make any definite conclusions the results are, in our opinion, interesting enough to publish in this paper.

The remainder of the paper is organized as follows: the next section gives some basic background on Cloud Computing. Section 3 provides

[1]Note that with regard to Cloud Computing, this paper is limited to Business to Business (B2B) Cloud Computing initiatives. Cloud Computing initiatives directed to consumers, such as Microsoft's Windows Live Mail or Google's Gmail are not part of this research.

an overview of several US and EU privacy regulations and Section 4 discusses the privacy regulations in relation to Cloud Computing. Next follows a more general discussion and the paper ends with conclusions.

2 Cloud Computing

Cloud Computing is a new paradigm in Information Technology (IT). In their research Vaquero et al. (2009) propose the following definition:

> Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization.

In traditional IT environments, clients connect to multiple servers located on company premises. Clients need to connect to each of the servers separately. In Cloud Computing clients connect to the Cloud. The Cloud contains all of the applications and infrastructure and appears as a single entity. Cloud Computing allows for dynamically reconfigurable resources to cater for changes in demand for load, allowing a more efficient use of the resources.

In Cloud Computing, end users are provided with dedicated hardware or a virtualized machine. To end users, this virtual machine appears as an isolated machine, where each user has isolated access. In Cloud Computing standardization has not yet emerged. Using software in a Cloud Computing environment therefore depends on the CSP. Virtualization in Cloud Computing allows distributing computing power to cater for load fluctuations. Standard web protocols provide access to Cloud Computing and control is centrally managed in various data centers.

Cloud Computing is offered through three types of services (Lin et al., 2009; Weinhardt et al., 2009). These services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Infrastructure as a Service (IaaS), sometimes referred to as Hardware as a Service (Wang et al., 2008), allows the use of hardware through commonly available interfaces, such as web interfaces (Leavitt, 2009; Weinhardt et al., 2009) Due to the ubiquity of the web and the abstraction these interfaces provide, access to IaaS is claimed to be simple and easy. Although some researchers place storage as a separate service (e.g. Grossman, 2009), we will not do this

and follows other researchers who define storage as a part of the IaaS concept.

Platform as a Service (PaaS) provides users with a platform to develop and execute software through similar interfaces as IaaS and SaaS. Developing software on PaaS allows users to collaboratively write the code and execute it in the Cloud.

Software as a Service (SaaS) provides users with applications that are easily accessible by providing common and ubiquitous interfaces. In contrast to normal applications, the applications in SaaS are installed on remote computers and not on the user's computer.

The three Cloud services of Cloud Computing are related. They can be consumed as separate services or can be combined. I.e. PaaS can be installed on IaaS (Lederman et al., 2008; Lin et al., 2009). This relationship is visually represented in Figure 1.

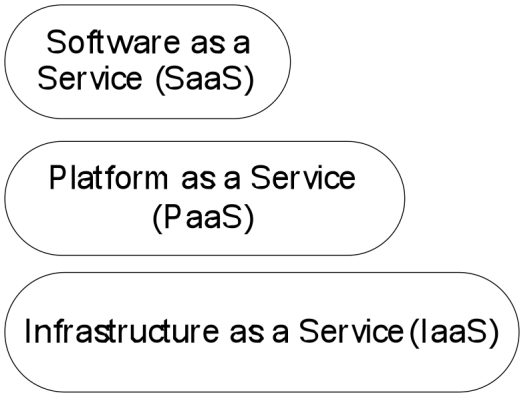

Figure 1: The Cloud service layers (adapted from Grossman, 2009; Lin et al., 2009 and Weinhardt et al., 2009)

Portraying the Cloud services in layers resembles the OSI stack that comprises traditional computing. At the same time the layers represent the amount of control users have over their Cloud Computing initiative. Each layer provides further abstraction to users of Cloud Computing. IaaS hereby offers the least abstraction and SaaS the most. With more abstraction, more control of the technology stack is taken away by the Cloud Service Provider or IT organization.

These cloud services can be obtained from 3rd parties, referred to as Cloud Service Providers (CSPs) (Armbrust et al., 2009; Vaquero et al., 2009). Organizations can also opt for Cloud Computing technology within their own datacenter (Grossman and Gu, 2009; Leavitt, 2009).

Cloud Computing technologies can be classified into four different types: public Clouds, private external Clouds, private internal Clouds and hybrid Clouds. Security aspects, interoperability, pricing and benefits of Cloud Computing depend on the type of Cloud. Table 1 provides an overview of the classification and its characteristics.

	Managed by	Owner of infrastructure:	Dedicated hardware
Public	Cloud Service Provider	Cloud Service Provider	No
Private, external	Cloud Service Provider	Cloud Service Provider	Yes
Private, internal	Internal Organization	Internal Organization	Yes
Hybrid	Mixed	Mixed	Depends on contract with the CSP

Table 1: Cloud Type classification

In a public Cloud, organizations use Cloud Computing technologies through a CSP. The Cloud is physically located outside the premises of the organization. The Cloud is fully outsourced to the CSP, leaving the organization with little direct control over the hardware (Grossman, 2009). Public Clouds are typically offered through virtualization and distributed among various physical machines. Often multiple Clouds are hosted on the same hardware.

In private external Clouds, Cloud Computing is still offered by a CSP. The difference between public Clouds and private external Clouds is found in the hardware. In public Clouds, hardware is shared among different Clouds. In private external Clouds, the hardware only hosts the Cloud of one customer. This provides more opportunities for better (physical) security.

In private internal Clouds, organizations use Cloud Computing technologies within the organization's data center (Grossman, 2009). Private internal Clouds allow organizations to use the scaling of resources Cloud Computing provides, without handing over any control to a CSP. Private internal Clouds allow the organization full control over the Cloud. Organizational hardware, software and security standards can be used without the need for concessions to a CSP.

Hybrid Clouds are a combination of the other Cloud types. In a hybrid Cloud, organizations use a CSP in cases where additional resources are required.

3 Privacy Regulations

This section provides an overview of the most important privacy regulations in the United States and the European Union that are applicable to Cloud Computing. Policies on the creation of privacy legislation in the European Union and the United States differ. The United States favor a more laissez-faire approach. Industry self-regulation is favored over federal law (Baase, 2007; Movius and Krup, 2009; Steinke, 2002). It is believed that businesses shape their policies according to consumer preferences, following economic theory. This theory implies that consumer preferences determine market share, and that a higher market share leads to higher profits (Strauss and Rogerson, 2002). The Payment Card Industry Data Security Standards (PCI-DSS), discussed below, is an example of a self regulation policy. In situations where self regulation fails, sector specific laws are created so that other sectors are not hindered (Movius and Krup, 2009; Strauss and Rogerson, 2002). The sector specific laws only apply to a specific sector and do not oppose self-regulation initiatives in other sectors.

Privacy in the United States is dispersed among various different sector specific laws (Sarathy and Robertson, 2003). This paper is limited to a selection of sector specific laws and focuses on the privacy aspects of these laws. These sectors include the health care sector for the Health Insurance Portability and Accountability Act (HIPAA) and the financial services sector for the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and the Payment Card Industry Data Security Standards.

The European Union has a different approach concerning legislation. The European Union approach to legislation favors participation among businesses and governments as opposed to the US self-regulation approach (Movius and Krup, 2009). The European Union set privacy regulations up front as opposed to relying on industry self regulation (Baumer et al., 2004; Movius and Krup, 2009; Steinke, 2002).

3.1 EU Directive 95/46/EC

Directive 95/46/EC, commonly known as the Data Protection Directive (Birnhack, 2008), was implemented in October 1995 (EU

Directive, 1995). The main purpose of the directive was to harmonize the privacy laws that existed in the different member states of the European Union and to provide a basic standard on privacy protection (Birnhack, 2008; EU Directive, 1995; Jentzsch, 2003).

Directive 95/46/EC addresses personal data, or personally identifiable information. Personal data is defined as any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Directive 95/46/EC consists of 32 articles setting requirements on handling personal data and mandating the countries of the EU to implement them (EU Directive, 1995).

The directive makes an implicit distinction between *data controller* and *data processor*. The data controller, the legal entity that chooses if and how data is processed, is responsible for compliance. It can choose to use a third party (the data processor) for data processing and should ensure that this is done in compliance with the directive. If the data processor resides in the EU and the data controller does not then it is the responsibility of the data processor to enforce the EU Directive 95/46/EC. Note that this is especially relevant in the context of cloud computing: all `European' clouds, i.e., running on hardware located in a EU member state, have to ensure compliance with the EU Directive 95/45/EC – even if the data controller is not an EU company.

Directive 95/46/EC was written with the purpose of safeguarding the privacy of European Union inhabitants and to integrate different privacy legislation of EU member countries. There are several ways of complying with Directive 95/46/EC. European based organizations should adhere to its principles. Organizations outside the EU may use the Safe Harbor Agreement, Standard Contractual Clauses or Binding Corporate Rules.

3.2 The Safe Harbor Agreement

From a European point of view, the United States do not provide adequate privacy protection. This prevents data transfers between Europe and the United States. To address this problem, the European Commission and the United States Department of Commerce negotiated the Safe Harbor agreement (Bull, 2001; Fromholz, 2000). The agreement aims to align the process for US companies to comply with the EU Directive 95/46/EC.

The Safe Harbor agreement is only applicable to transfers between the United States and the European Union. Organizations outside the United States that have business operations within the European Union, have to rely on different mechanisms to adhere to the Transborder Transfer principle from Directive 95/46/EC. This principle requires that personal identifiable information can only be transferred to those countries that are deemed to provide adequate security. A US-based organization can adhere to the principles of the Safe Harbor agreement which guarantee (i) notice if data is collected, (ii) choice for individuals to opt-out of the collection of data, (iii) no transfer of collected data unless explicitly consented to by an individual, (iv) security of the collected data, (v) integrity of the collected data, i.e., the data should be factual and accurate, (vi) individuals have the right to access data held about them and (vii) the above rules must be enforced. An example (Cloud Computing) company that is safe harbor compliant is Google.

The Safe Harbor agreement provides a substitute for adequate protection. In order to comply with the Safe Harbor agreement an organization must follow the Safe Harbor Privacy Principles, disclose their privacy policies, be subject to the statutory powers of the Federal Trade Commission, verify compliance with the Principles through self- or third-party assessment and register with the Department of Commerce. The Department of Commerce maintains a list with organizations adhering to the Safe Harbor agreement.

There is a substantial difference in European and US privacy regulations: European privacy laws apply only to personal data, i.e. data of a natural person whereas in the US, there is something like a privacy of a legal person.

Related to the Safe Harbor agreement are the Binding Corporate Rules (BCRs). These are sometimes presented as an alternative to the Safe Harbor Agreement. This is not the case (Bender and Ponemon, 2006). BCRs are used to ensure a form of complience to EU rules *inside* an organization for transfer from the EU to any other country (not just the USA). The rules do provide a form of certification for the complaince of a company to the EU data directive, and thus give an indication of safe harbor compliance.

3.3 The FTC Fair Information Practice

The FTC Fair Information Practice forms a set of guidelines concerning fair use of information about individuals. They originated in 1973 in the US Secretary's Advisory Committee on Automated

Personal Data Systems. The Federal Trade Commission (FTC) first mentioned its Fair Information Principles in the 1998 report Privacy Online: A Report to Congress (Annecharico, 2002). The latest version has been published by the FTC on the 25th of June 2007. Organizations are encouraged to adhere to the Fair Information Practice but cannot be enforced to comply with the principles.

The FTC Fair Information Practice have their roots in privacy principles in the United States, Canada, and Europe, including Directive 95/46/EC. The FTC Fair Information Practice consist of the following five principles portrayed (i) Notice/Awareness, (ii) Choice/Consent, (iii) Access/Participation, (iv) Integrity/Security and (v) Enforcement/Redress

These principles are basically the same as the principles in Directive 95/46/EC, with the exception of the Transborder Transfer principle (though similar principals could be added for other countries). The Integrity and Security principle are combined into a single principle. The Enforcement principle calls for self-regulation, organizations are not mandated to comply with the FTC Fair Information Practice.

3.4 Other Privacy Regulations

Some other American privacy regulations are sector specific, they include (i) the Health Insurance Portability and Accountability Act (HIPAA) which is created specifically for the health industry, (ii) The Gramm-Leach-Bliley Act (GLBA) which is specifically designed for the financial services sector and applies to financial institutions (see Section 4 for a more thorough discussion of these acts) and (iii) the Fair Credit Reporting Act (FCRA) applies to consumer reports of United States citizens. The Act covers Credit Reporting Agencies (CRAs) and is enforced by the Federal Trade Commission. All these acts basically implement the Fair Information Principles discussed in Section 3.3.

Another act that is relevant in this context is the United Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act. It differs from other legislation this paper addresses. The USA-PATRIOT can be seen as a law limiting privacy, opposed to the other privacy preserving regulations addressed (Baase, 2007).

The USA-PATRIOT Act is compliant with none of the Fair Information Practice Principles and the principles found in Directive 95/46/EC. The Act, particularly in sections 215 and 505, allows for the collection of information without consent of the individual. Reasons for information collection are not completely disclosed. Secondary use of

the information is allowed under 'domestic terrorism' reasons. There is a lack of clarity regarding the purpose of information collected, which makes it impossible to evaluate relevance and data quality. Accountability is absent on the part of those collecting and disclosing information (Regan, 2004). Note that, while there is no equivalent for the USA-PATRIOT act in a European context, individual police and secret services have similar possibilities for using wiretaps etc. thus also potentially hindering privacy is this context.

The Payment Card Industry – Data Security Standard (PCI-DSS) is an example of industry self regulation. The payment card industry has set compliance with the PCI-DSS as mandatory for organizations handling and processing payment card transactions (Wright, 2008).

The main privacy provisions of the PCI-DSS specifically address data related to card holders. These include (i) the requirement to protect cardholder data, (ii) the requirement to encrypt transmission of cardholder data across open, public networks, (iii) the development and maintenance of secure systems, (iv) access restriction to cardholder data by businesses on a need to know basis, (v) physical access restriction to cardholder data and (vi) the creation of a policy to increase employee awareness on compliance with the PCI-DSS.

3.5 Common Principles in Privacy Regulations

The privacy regulations discussed in this section have much in common, with the notable exception of the USA-PATRIOT act. The principles of Directive 95/46/EC and the FTC Fair Information Practice Principles are stated in similar terms. Additionally, it is said these principles are recognized worldwide as setting the standard for privacy (Movius and Krup, 2009; Regan, 2004). These principles therefore provide a standard in comparing privacy regulations. This comparison is shown in Table 2.

	FTC Fair Information Practice Principles	Directive 95/46/EC	The HIPAA	The Gramm-Leach-Bliley Act	The Fair Credit Reporting Act	PCI-DSS
Notice	√	√	√	√	√	
Choice/Consent	√	√	√	√	√	
Access	√	√	√		√	
Integrity	√	√	√	√	√	√
Security	√	√	√	√		√
Enforcement	√	√	√	√	√	√

Table 2: Common principles in privacy regulations

The horizontal axis states various privacy laws and regulations. A check means the principle is present in the regulation. The vertical axis portrays the common principles in the various privacy laws and regulations. This overview shows that the various privacy regulations are similar in nature. Nearly all the regulations provide individuals with a notice of the use of information, a form of consent for use of the information, require access to his/her data, require the integrity and security of the data and set demands for enforcement.

4 Privacy Issues for Cloud Service Providers

This section tries to identify the scope and applicability of the privacy regulations from the previous section regarding the Cloud Computing paradigm. An important aspect in enforcing privacy regulations is the physical location of an organization's Cloud Computing initiative. A CSP hosts an organization's Cloud Computing initiative in a distinct physical location. It is currently unknown what the consequences of local legislation on the Cloud's physical location are. Several researchers expect jurisdictional conflicts to arise (Jaeger et al., 2009; Mowbray, 2009). To place these jurisdictional conflicts in the scope of this paper; it is currently unknown if e.g. the Health Insurance Portability and Accountability Act (HIPAA) applies to a European health-care organization outsourcing health care data to a CSP located in the United States.

When organizations have a legal obligation to comply with legislation, these organizations are responsible and accountable for compliance (Eisenhauer, 2005; Lewis, 2009). Organizations can be held liable if a subcontractor breaches compliance with legislation. It is

unknown if a CSP is legally considered the same as a subcontractor. Currently there is no jurisprudence on this matter. However, it is claimed that a CSP can be legally seen as a subcontractor (Gellman, 2009). This implies that organizations should ensure that a CSP is compliant with relevant privacy legislation. Various governments have posed laws, which require access to data stored in their jurisdiction for electronic discovery or anti-terrorism purposes (Gellman, 2009; Jaeger et al., 2008). An example of such a law can be found in the USA-PATRIOT Act. In most cases a form of subpoena or search warrant is required to provide a government legal authority to access stored data. The response to a search warrant or subpoena to a CSP differs per CSP (Soghoian, 2009). Some CSPs may object to the subpoena, others may comply without hesitation.

Cloud Computing offers the ability to dynamically reconfigure computing resources as demand for computing resources increases or decreases. A CSP needs to be capable of provisioning this demand. In cases where a CSP fails to provision this demand, the CSP itself may be forced to outsource organizational data to a different CSP, amplifying the location related privacy issues portrayed above.

With the exception of the USA-PATRIOT Act, all regulations addressed in Section 3 forbid secondary uses of covered data without consent from the data subject. A CSP may have the potential to use the data provided by an organization. Researchers have mentioned the potential of using this data for marketing and data mining purposes (Jaeger et al., 2008). When a CSP processes or transmits organizational data for purposes other than specified at the time an organization collected the data, the organization is no longer compliant to the corresponding privacy regulation.

In Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) privacy issues pertaining to government access and secondary uses of data can be circumvented by use of encryption (Mowbray, 2009). For example, users can store their information in the cloud in encrypted form which prevents CSPs from accessing this data. In Software as a Service (SaaS) initiatives the use of encryption may not provide a solution to government access and secondary use of data. In SaaS the CSP actively processes organizational data in order to deliver its service. Encrypting data potentially renders the data unsuitable for processing by the CSP. State of the art encryption methods can counter this effect. For example, when using homomorphic encryption (Gentry,

2009) CSPs can still process the data without accessing the content, thus CSPs and governments will not be able to decrypt this data[2].

4.1 The CSP and Privacy Regulations

None of the regulations described in Section 3 specifically mentions how using services offered by a CSP impacts compliance with the regulation. With the exception of the PCI-DSS, all regulations were created before the term Cloud Computing emerged. How Cloud Computing affects compliance with regulations is therefore subject to debate.

Solutions for compliance with pro-privacy regulations are given by several CSPs. A number of CSPs adhere to the Safe Harbor agreement. Adherence to the Safe Harbor agreement signifies compliance with Directive 95/46/EC. Examples of CSPs adhering to the Safe Harbor Agreement are Amazon, Google and Salesforce.com. Adherence to the Safe Harbor agreement obligates the CSP to adhere to several principles. These principles are the same principles as outlined in Section 3. The contents of the principles found in the Safe Harbor agreement resemble the FTC Fair Information Practice Principles.

The HIPAA act requires organizations subject to compliance to set up a business associate agreement with 'Business Associates'. A Business Associate is defined as 'a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.' (HIPAA, 1996) In plain terms, a business associate is a third party, i.e., an employee of another company, performing services related to the organization that involved Public Health Information (PHI). When a third party merely acts as a conduit, for example a postal service, the third party is not categorized as a Business Associate. It is believed CSPs should be regarded as Business Associates. Gelmann states that: 'A conduit transports information but does not access it except infrequently as necessary for the performance of the service, or as required by law. In theory, a cloud provider could possibly be a conduit for HIPAA purposes, but much depends on the terms of service. If the cloud provider reserves any

[2]Note that in various jurisdictions it might be illegal to keep relevant encryption keys from law enforcers. For example see Part 3, Section 49 of the United Kingdom's Regulation of Investigatory Powers Act (RIPA, 2000).

rights to review, use, disclose, or post information submitted by a user, the provider will not qualify as a conduit' (Gellman, 2009).

The Financial Privacy Rule and Safeguards Rule of the Gramm-Leach-Bliley Act (GLBA) specifically mention service providers. Organizations striving for GLBA compliance need to take certain precautions when engaging in a business relationship with a service provider. The Financial Privacy Rule of the GLBA mandates organizations to hand out a notice to their clients stating the disclosure of the clients' Non-Public Information (NPI) to a service provider. The exchange of NPI with a service provider requires a contract. This contract should state the confidentiality of the NPI by guaranteeing the data is only used for the purpose for which it was shared. The Safeguards rule of the GLBA requires organizations to only select service providers capable of maintaining appropriate safeguards. A contract with the service provider should be established, requiring the service provider to maintain the appropriate safeguards. Organizations are required to ensure service providers comply with the contract. Furthermore organizations should oversee the handling of NPI by service providers.

The Fair Credit Reporting Act (FCRA) allows the sharing of consumer reports after the provision of the credit report to the related individual and an option to opt-out on the sharing (FTC, 2009).

Although the Payment Card Industry Data Security Standards (PCI-DSS) were created after the introduction of Cloud Computing, a CSP is not specifically mentioned in the PCI-DSS. The PCI-DSS gives a notion of general service providers. A service provider is defined as a 'Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, intrusion detection systems and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.' (PCI, 2009) If a CSP is seen as a service provider depends on the interpretation of the term 'directly involved'. When a CSP is directly involved in processing, storage, or transmission of cardholder data it is seen as a service provider. In this case, an organization engaging in a business relationship with a CSP needs to assure the CSP is compliant with the PCI-DSS. If a CSP is not 'directly involved' in the processing, storage or transmission of

cardholder data, the organization engaging in a business relationship with a CSP needs to clearly define which PCI-DSS requirements are handled by the CSP. The CSP then has two options to assure compliance with the PCI-DSS: undergo a PCI-DSS assessment themselves, or have their services reviewed during the course of each of their customer's PCI-DSS assessments. In general, it is assumed that CSPs adhere to the definition of service provider. Several CSPs assure PCI-DSS compliance by being compliant with the PCI-DSS themselves. Examples of PCI-DSS compliant CSPs are Aria Systems and OpSource. VISA Inc. maintains a list of PCI-DSS approved organizations (VISA, 2009). Organizations wishing to adhere to the PCI-DSS can confirm the compliance of their Cloud Computing initiative by verifying that the proposed CSP is mentioned on the VISA list and verifying the scope of the compliance.

This section addressed some of the privacy issues posed by Cloud Computing. The biggest threat to privacy in Cloud Computing is posed by outsourcing personal data to a CSP. The CSP is in physical control over data hosted within the Cloud Computing initiative while the accountability for non-compliance with privacy regulations lies with the CSPs client. The location in which the CSP physically hosts the data may pose issues with regulatory compliance. Another issue caused by the CSP is the disclosure of data to other non-affiliated third parties such as governments or marketing bureaus.

5 Privacy Regulations in Theory & Practice

This paper intends to provide clarity on the impact of Cloud Computing on privacy regulations and the impact of privacy regulations on Cloud Computing. An extensive literature study in combination with interviews with ten CSPs[3] (Ruiter, 2009) highlights several points of discussion:

- *Information security in Cloud Computing consists of established security solutions such as encryption, access management, firewalls and intrusion detection*. In internal Clouds the IT department has the ability to install all available security solutions it sees fit. In external Cloud Computing the security

[3] The size of the CSPs contacted ranged from startup companies to several large-scale service providers. The CSPs provided answers to these questions on the condition of anonymity. We realize the results are not conclusive (nor repeatable), but they give an indication of how CSPs currently address privacy issues.

depends on the Cloud Service Provider (CSP). Some CSPs do not provide flexibility in the choice of security solutions, while others allow the implementation of client security requirements. The amount of control over the security depends on Cloud service. In IaaS, where clients are able to virtually manage an infrastructure, clients are usually able to implement more security measures than in SaaS, in which clients only use a software solution. Not all CSPs allow client-auditing of their security offerings. In these cases client organizations have to suffice with a CSP-provided audit statement, mostly SAS70 - Type II (SAS70), or have to take the CSPs word on the level of provided security.

- *Data storage, transmission and processing in Cloud Computing depends on the Cloud type, e.g. internal or external Cloud Computing, and the service, i.e., IaaS, PaaS, or SaaS*. In private, internal Cloud Computing the organization keeps all data within its own datacenter. Through techniques such as service-oriented computing and virtualization, the datacenter offers the benefits associated with Cloud Computing: faster and more efficient allocation of resources. In external Cloud Computing data is outsourced to a CSP. How the data is transmitted to the CSP depends on the CSP itself. Some CSPs allow encrypted data transmission, others do not. The storage of data dependents on the CSP as well. Some CSPs encrypt data or outsource data storage to a different CSP. It is unknown whether data is encrypted during the transfer between CSPs. Processing of data entirely depends on the CSP and the service. SaaS providers offer a specific processing service, whereas in IaaS the client organization determines to a large extent how the data is processed. CSPs may offer completely different services, thereby processing data in completely different ways.
- *The impact of privacy regulations is most dramatic between external Cloud Computing and traditional IT*. In external Cloud Computing, data gets outsourced to a CSP. The CSP has physical control over the Cloud Computing initiative while the accountability for non-compliance with privacy regulations lies with the CSPs client. Another issue in is related to the physical location where the CSP hosts the Cloud. The Transborder Transfer principle in Directive 95/46/EC requires organizations to exchange data only to countries that provide adequate protection. If an organization does not know where its data is

hosted, this principle might be violated. Data location could also be an issue under local laws. It is unknown if local regulations regarding data apply to the physical location of the Cloud. Another issue caused by the CSP is the potential disclosure of data to other non-affiliated third parties such as governments or marketing bureaus, i.e., use of data. Directive 95/46/EC, the FTC Fair Information Practice Principles, the Health Insurance Portability and Accountability Act (HIPAA) and Fair Credit Reporting Act (FCRA) all require that data only gets used in the purpose for which it was collected. In the Gramm-Leach-Bliley Act (GLBA) this requirements holds for data received indirectly; i.e. the CSP getting the data from its client organization.

- *The concept of Cloud Computing brings many uncertainties with respect to compliance with privacy regulations*. There are no clear answers on which privacy regulation requirements apply to Cloud Computing; none of the regulations from Section 3 explicitly mention Cloud Computing. The absence of cases in which an organization is accused of not being compliant with privacy regulations does not provide clarity either. There are only few case studies known in literature that describe HIPAA compliance in Cloud Computing. These cases leave several questions unanswered and do not provide enough information on the way certain regulatory requirements are implemented within the Cloud service. In general, the CSPs participating in the interviews from (Ruiter, 2009) do not know whether or not they are compliant with privacy regulations. A few notable exceptions are CSPs that are compliant with the Safe Harbor Agreement or have done PCI-DSS compliance audits themselves. This seems to be the only way in assuring compliance with privacy regulations: selecting CSPs which are compliant themselves. In those cases where CSPs are compliant with regulations, it is certain privacy regulations have affected the implementation of Cloud Computing: The services offered by the CSP are designed in such a way that compliance can be assured. In other cases the impacts of privacy regulations on Cloud Computing are not fully known.
- *Security is seen as a major issue in the adaptation of Cloud Computing, compliance to privacy regulations is not*. The interviews from (Ruiter, 2009) seem to indicate that CSPs in general do not know if they are compliant with privacy regulations. Customers seem to only inquire about the security of

the Cloud, not about privacy regulations. One of the CSPs participating in the questionnaire stated privacy regulations did not influence the design of the security solutions at all. By combining these results, it seems privacy regulations have little influence on the security design of Cloud Computing. An exception to this rule are the CSPs' compliant with the PCI-DSS. The PCI-DSS sets standards on data security. PCI-DSS compliant CSPs have assured their security design/architecture is sufficient in adhering to the PCI-DSS.

- *It looks like many organizations are simply not aware of privacy issues in Cloud Computing (Ruiter, 2009).* Clients of the corresponding CSPs in general do not inquire about compliance with privacy regulations when establishing a business relationship with the CSP. Compliance with most regulations is mandatory. Therefore it seems organizations are not aware of the effects outsourcing data to a CSP may have with respect to compliance or that they think the issues are not important.

Privacy regulations are clearly not enough to solve all the privacy issues related to Cloud Computing. Raising awareness about both the issues and the existing regulations seems a good first step to remedy this.

6 Conclusions

There are still many uncertainties with respect to privacy regulations and Cloud Computing. There are very few case studies that concern compliance of privacy regulations with respect to Cloud computing in literature. The case studies that do exist do not clearly indicate how specific regulatory issues are handled. Non-compliant cases are nowhere to be found in literature. In general, CSPs seem to be unsure on how they should be handling privacy requirements. It is not possible to provide complete certainty on how organizations should implement Cloud Computing. The only way to provide certainty is when the CSP itself complies with the regulations. Adhering to the Safe Harbor agreement ensures compliance with Directive 95/46/EC. Several CSPs are adhering to the PCI-DSS as well. The ability to create HIPAA compliant Clouds is given by a couple of CSPs as well.

Even when the CSP is compliant with the privacy regulations, client organizations still need to make sure they adhere to the principles set in the various regulations themselves. More awareness amongst client organizations may eventually lead to more and better compliant CSPs.

We believe that research in the fields of privacy legislation and Cloud Computing would benefit substantially if future researchers could have access to more case studies addressing Cloud Computing. This could provide practical examples on how implementation of Cloud Computing affects the compliance of organizations with privacy regulations. Part of such research should be performed by people with sufficient knowledge of IT and legal practice. A legal background is required in order to determine the best way to interpret of regulations when applied to Cloud Computing. It is the opinion of the authors that due to the case law found in the United States, full clarity compliance can only be given when alleged non-compliance is brought to Court or when government officials create Cloud Computing specific legislation.

Acknowledgements The authors would like to thank Shay Uzery and Accenture for making this research possible. We also like to thank the anonymous reviewers for many suggestions that helped to improve the overall quality of the paper.

References

Annecharico, D. (2002). Notes & Comments: V. Privacy after GLBA: Online Transactions: Squaring the Gramm-Leach-Bliley Act Privacy Provisions With the FTC Fair Information Practice Principles. *NC Banking Inst. 6*, 637–695.

Armbrust, M., A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al. (2009). Above the clouds: A berkeley view of cloud computing. *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28*.

Baase, S. (2007). *A gift of fire: Social, legal, and ethical issues for computing and the Internet*. Prentice Hall.

Baumer, D., J. Earp, and J. Poindexter (2004). Internet privacy law: A comparison between the United States and the European Union. *Computers & Security 23*(5), 400–412.

Bender, D. and Ponemon, L (2006). Binding Corporate Rules for Cross-Border Data Transfer. *Rutgers Journal of Law & Public Policy*

Birnhack, M. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Report 24*(6), 508–520.

Bull, G. (2001). Data Protection - Safe Harbor, Transferring Personal Data To The USA. *Computer Law & Security Report 17*(4), 239–243.

Eisenhauer, M. (2005). Privacy and Security Law Issues in Off-shore Outsourcing Transactions. *Hunton & Williams, Atlanta Georgia 15*.

EU Directive (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Fromholz, J. (2000). European Union Data Privacy Directive, The. *Berk. Tech. LJ 15*, 461.

FTC (2009). Federal Trade Commission, Fair Credit Reporting Act.

Gellman, R. (2009). WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. *Released February 23*.

Gentry, C. (2009). *A fully homomorphic encryption scheme,* Phd Thesis, Standford University.

Grossman, R. (2009). The Case for Cloud Computing. *IT Professional 11*(2), 23–27.

Grossman, R. and Y. Gu (2009). On the Varieties of Clouds for Data Intensive Computing. *Data Engineering*, 44.

HIPAA (1996). Health Insurance Portability and Accountability Act of 1996.

Jaeger, P., J. Lin, and J. Grimes (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics 5*(3), 269–283.

Jaeger, P., J. Lin, J. Grimes, and S. Simmons (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday 14*(5-4).

Jentzsch, N. (2003). The regulation of financial privacy: the United States Vs Europe. *ECRI Research Report 5*.

Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time? *Computer 42*(1), 15–20.

Lederman, L., B. Suri, J. Houston, and S. Itchhaporia (2008). *The Next Stage of Computing*. William Blair & Company.

Lewis, S. (2009). Cloud Computing Brings New Legal Challenges. *New York Law Journal*.

Lin, G., D. Fu, J. Zhu, and G. Dasmalchi (2009). Cloud Computing: IT as a Service. *IT Professional 11*(2), 10–13.

Movius, L. and N. Krup (2009). U.S. and EU Privacy Policy: Comparison of Regulatory Approaches. *International Journal of Communication*, 169–187.

Mowbray, M. (2009). The Fog over the Grimpen Mire: Cloud Computing and the Law. *Script-ed Journal of Law, Technology and Society 6*(1).

PCI (2009). PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures version 1.2.

Regan, P. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly 21*(4), 481–497.

RIPA (2000). United kingdom. regulation of investigatory powers act.

Ruiter, J. (2009). The Relationship between Privacy and Information Security in Cloud Computing Technologies. Master's thesis, Vrije Universiteit Amsterdam.

Sarathy, R. and C. Robertson. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business ethics 46*(2), 111–126.

SAS70. American Institute of Certified Public Accountants, Statement on Auditing Standard 70.

Soghoian, C. (2009). Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era.

Steinke, G. (2002). Data privacy approaches from US and EU perspectives. *Telematics and Informatics 19*(2), 193–200.

Strauss, J. and K. Rogerson (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics 19*(2), 173–192.

Vaquero, L., J. Caceres, M. Lindner, and Rodero-Merino (2009). A Break in the Clouds: Towards a Cloud Definition. *ACM SIGCOMM Computer Communication Review*, 50–55.

VISA (2009). VISA Inc, Global List of PCI DSS Validated Service Providers.

Wang, L., G. von Laszewski, M. Kunze, and J. Tao (2008). Cloud Computing: a Perspective Study. *Service Oriented Cyberinfrastruture Lab, Rochester Inst. of Tech–Dezembro de*.

Weinhardt, C., A. Anandasivam, B. Blau, and J. Stosser (2009). Business Models in the Service World. *IT Professional 11*(2), 28–33.

Wright, S. (2008). *PCI DSS: A Practical Guide to Implementation*. IT Governance Ltd.