On the Relationship between the Different Methods to Address Privacy Issues in the Cloud

Siani Pearson

Security and Cloud Lab, HP Labs, Bristol, UK
Siani.Pearson@hp.com

Abstract. In conjunction with regulation, information security technology is expected to play a critical role in enforcing the right for privacy and data protection. The role of security in privacy by design is discussed in this paper, as well as the relationship of these to accountability. The focus within these discussions is on technological methods to support privacy and data protection in cloud scenarios.

Keywords: Accountability, Cloud Computing, Design for Privacy, Security.

1 Introduction

Privacy in cloud business environments can be a difficult issue to tackle because of the underlying complexity across multiple dimensions and the interdisciplinary nature of the problem. For example, location matters from a legal point of view but processing flows are dynamic, global and fragmented: there are restrictions about how information can be sent and accessed across boundaries, but in cloud computing data can flow along chains of service providers both horizontally between Software and a Service (SaaS) providers and vertically, down to infrastructure providers, where the information can be fragmented and duplicated across databases, files and servers in different jurisdictions. However, data controllers still have the responsibility to ensure that the service providers are meeting regulatory obligations.

In this paper the overarching means of addressing privacy issues in cloud computing are analysed, with a focus on privacy by design, security and accountability. The relationship between such notions is a complex one that has not been sufficiently elucidated to date. This paper examines that relationship, including the following issues:

- to what extent is information security an integral part of privacy by design?
- what is the relationship of accountability to privacy by design?
- how does this apply in the cloud context?

The importance and timeliness of this analysis is underpinned both by technological and business changes embodied within the adoption of cloud computing that need to be deployed in such a way as to reduce privacy risk, as well as ongoing global regulatory changes. Notably, problems with the 1995 EU Data Protection Directive [1]

R. Meersman et al. (Eds.): OTM 2013, LNCS 8185, pp. 414–433, 2013.
© Springer-Verlag Berlin Heidelberg 2013

as a harmonisation measure and in relation to new technologies including cloud computing have led the European Commission (EC) in January 2012 to publish a draft of replacement General Data Protection Regulation that is currently being discussed and revised [2], in which accountability features and privacy by design take greater precedence. Amongst other things, this imposes new obligations and liabilities for data processors, new requirements on data breach notification and stricter rules on international data transfers. It also empowers National Regulatory authorities to impose significantly higher fines.

The structure of this paper is as follows: section 2 highlights some key privacy challenges for the cloud and general categories of mechanism by which these may be addressed; section 3 and 4 then consider some of the key relationships between these, notably to what extent information security is an integral part of privacy by design, and the relationship of accountability to privacy by design, and how this applies in a cloud context. Finally, conclusions are given.

2 Cloud Privacy Issues: Do We Have All the Answers?

In this section key cloud-related terminology is introduced, cloud privacy issues are discussed and generic approaches to tackle these problems are introduced. What makes data processing in the cloud challenging is the rapidly expanding scale of cloud services, the pervasive role they will play in the future business and personal life, the complexity of the supply chain and the ability of advanced data mining techniques to draw inferences about data subjects from the large datasets under their control. The ‘data-centric’ nature of cloud computing creates a tension between service suppliers who perceive that the data they hold could be a strategic business resource and their customers who are increasingly aware of risks posed by the perceived lack of control over data in the cloud. The actual level of control in the cloud can be very variable. Transparency, remediation, clarification of responsibilities and maintenance of obligations within the supply chain are all key issues.

2.1 Cloud Computing

A definition of cloud computing that is commonly accepted is provided by the United States National Institute of Standards and Technologies (NIST): “*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*” [3]

There are different layers of cloud services that refer to different types of service model, each offering discrete capabilities. The service offered may be the delivery of computing resources such as storage and computing power, where the customer rents virtual machines from the service provider rather than buying hardware and software to provide these resources in the customer’s own data centre (this is known as Infrastructure as a Service, or IaaS), the delivery of a solution stack for software developers (Platform as a Service, or PaaS) or the delivery of software applications available on demand and paid for on a per-use basis (Software as a Service, or SaaS). These can be layered and combined in different ways. In addition there are several deployment models for cloud computing, of which the main ones are the following:

- **Private:** a cloud infrastructure operated solely for a single organisation, being accessible only within a private network and being managed by the organisation or a third party
- **Shared:** a cloud that is open to use by selected organisations
- **Public:** a publicly accessible and shared cloud infrastructure. In such an offering the stored data of different customers will usually be logically segregated
- **Hybrid:** a composition of two or more clouds that remain separate but between which there can be data and application portability

2.2 Cloud Privacy Challenges

There are a number of privacy-related challenges in the cloud, that include aspects such as whether data handling is compliant with laws and regulations, whether data is safe across all the cloud and under control throughout its lifecycle, whether data is handled based upon users' expectations, and whether appropriate use and obligations are ensured along the processing/supply chain. In this section further elucidation is given about some of these issues, with emphasis on aspects that are exacerbated or specific to cloud.

Table 1. Cloud Features and Key Related Privacy Issues

Cloud features	Key related issues
Multi-tenancy	Data of co-tenants may be revealed in investigations, isolation failure, proper deletion of data and virtual storage devices
Complex, dynamically changing environment; data flows tend to be global and dynamic	Ensuring appropriate data protection, overlapping responsibilities in data management, unauthorized secondary usage, vendor demise, lack of transparency
Data duplication and proliferation; Difficult to know geographic location and which specific servers or storage devices will be used	Exacerbation of trans-border data flow compliance issues, detecting and determining who is at fault if privacy breaches occur
Easy and enhanced data access from multiple locations	Data access from remote geographic locations subject to different legislative regimes, subpoenas, access by foreign governments, 'idiot with a credit card'

Cloud Features and Privacy Problems. Cloud vulnerabilities are varied and are categorised in material including [4]. Table 1 highlights some cloud features and associated potential issues, many of which are at the governance level. Data duplication and proliferation (and its autonomic aspect) creates problems in terms of compliance:

Amazon for example creates up to three copies in different data centres when storing data. In addition, public cloud providers make it very easy to open an account and begin using cloud services, and that ease of use creates the risk that individuals in an enterprise will use cloud services on their own initiative, without due consideration of the risks and due governance process. There are also fears, among users, about increased access to data by foreign governments and other parties. Other issues include data lifecycle management across chains of suppliers, including data discovery and destruction, and legal risks that include security obligations, international transfers and the processing of sensitive data. For example, difficulties exist if users want to end a service, get their data deleted or export their data to another provider. Often, it is unclear who the data controller is and which parties have what responsibilities. More detailed analysis is given for example in [5,6]. In particular, loss of control and transparency (in the sense of insufficient information, thus making the task more difficult of selecting a suitable service from the vast choice of cloud offerings) are highlighted as key issues by the Article 29 Working Party [7].

A Challenge in the Enterprise Security Life Cycle. All enterprises operate a security lifecycle something like the following: assess risk associated with IT; shape investment, controls and policy choices; applications and technical procurement; work hard to configure and patch the infrastructure environment; monitor events to catch incidents and support forensics; carry out audits to see if the controls are mitigating risks. Organisations struggle to operate this cycle effectively because: technology is always changing; threats and attacks evolve faster; the cycle consists of many silos of stakeholders that have very different perspectives and expertise and do not speak the same language. For example, legal or human resources employees involved in people policies are very different from a network security expert configuring firewalls. With cloud this situation is going to get even worse, not just because there are new architectures but because the supply chain of services breaks up the activities of the security lifecycle even further (as shown in Figure 1) [8].

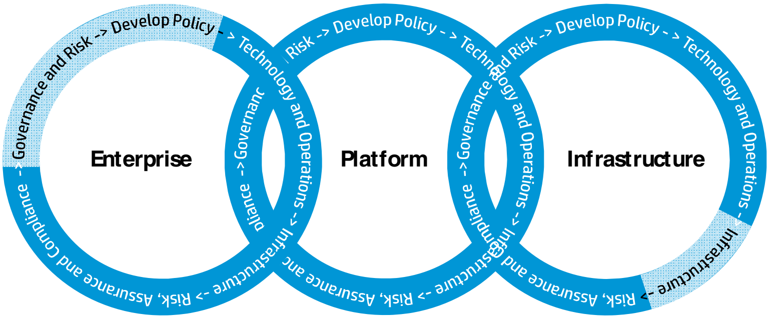

Governance and Risk -> Develop Policy -> Technology and Operations -> Infrastructure -> Risk, Assurance and Compliance ->
Enterprise
Platform
Infrastructure

Fig. 1. The Need for Accountability and Transparency in the Cloud Service Provision Chain

For instance, if the enterprise buys Customer Resource Management from a SaaS provider that in turn uses an Amazon Web Service for IaaS, then the people judging risks and forming policy now have to rely on and influence the investment and monitoring choices of the SaaS provider, and are also dependent on the configuration and infrastructure purchases of the IaaS. Hence there is a need for data stewardship and accountability along the service provision chain.

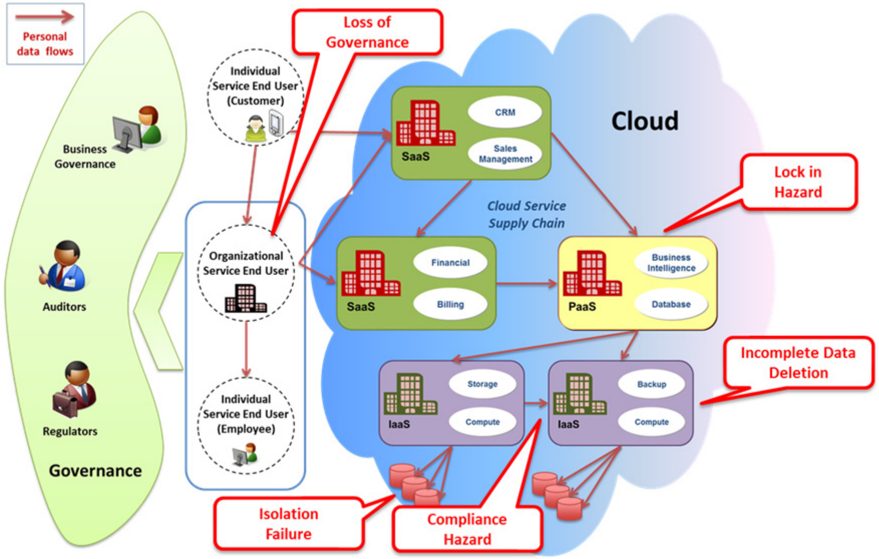


Fig. 2. Ramifications of Cloud Failures

Issues from one Cloud Service Provider (CSP) may have ramifications further up the chain, for example in terms of loss of governance. This is illustrated in Figure 2, which shows an example cloud ecosystem. Loss of governance may arise in cloud computing for example as the client cedes control to the CSP, but Service Level Agreements (SLAs) may not offer commitment to provide such services on the part of the CSP, thus giving a gap in security. There are many ways in which there can be data loss or leakage involving IaaS, PaaS and SaaS providers: for example, unauthorized parties might gain access to sensitive data due to insufficient authentication and authorization controls, or data might be stored in servers in India without appropriate governance mechanisms in place, causing a compliance hazard (for other examples see for instance [5]). Security and privacy threats of data breaches are the most severe types for cloud computing [9]. Unfortunately, some of the measures (e.g. data encryption) that can address data breaches may exacerbate data loss (e.g. if the encryption key is lost all encrypted data will be lost too). Data can be exposed to different types of security and privacy concern, and these include internal cloud facing security issues such as security attacks exploiting vulnerabilities of virtualization mechanisms and monitoring virtualized environments giving information about data usage by neighbouring users. Data breaches need to be addressed within specific provisions of

SLAs that clarify the respective commitments of the CSP and the client. An analysis of cloud failures has identified further threats (i.e. hardware failure, natural disaster, service closure, cloud-related malware and inadequate infrastructure planning) specific to cloud computing [10].

Security and Privacy Responsibilities in the Cloud. Security and privacy requirements in the cloud will vary widely from one use case to the next, and be heavily dependent upon risks and responsibilities of actors in those use cases, which again depend upon a combination of the service and deployment models used. For example, an internal private cloud can potentially offer an organisation greater oversight and authority over security and privacy, and better limit the types of tenants that share platform resources, reducing exposure in the event of a failure or configuration error in a control [11].

The NIST Cloud Computing Reference Architecture identifies the main roles in cloud computing [12]. Overall, SLAs define the respective responsibilities, although certain responsibilities are set by law, as discussed further below.

In terms of service models, the security that the consumer is responsible for will vary: the lower down the stack the cloud provider stops, the more security the consumer is responsible for implementing and managing [5]. In IaaS and PaaS, a great deal of orchestration, configuration and software development is performed by the customer, so much of the responsibility cannot be transferred to the CSP. Although the cloud provider bears most of the responsibilities for SaaS (normally being responsible for operational security processes i.e. user and access management, including identity management, authentication and compliance with data protection law), the virtual machine that contains licensed software and works with sensitive data places many more responsibilities on the consumer that builds and manages it. There is also potential for user responsibility to be outsourced to third parties who sell speciality security services, such as configuration management or firewall rule analysis.

2.3 Solutions

The following means can be used in combination in order to address the challenges above:

- *General standards and practices for operating in the cloud.* Several already exist, for example those provided by ENISA [4], CSA [5] and NIST [11]. The need for provision of consolidated European cloud standards has been highlighted and is currently being addressed within recent EC planning, as considered further in section 4.
- *Privacy by design.* Organisations need to think upfront about the impact and risks they create, and balance innovation with the expectations of individuals. A number of different techniques are available that can be used in combination to achieve this, and to provide data minimization, including anonymisation.

- *Security.* In the context of privacy, security relates to the protection of personal information. Many security controls are available in the cloud context: see for example the Cloud Controls Matrix mapping carried out by the CSA [13].
- *Accountability.* Broadly speaking this term is used in the sense here of corporate data governance related to personal data, including consideration of responsibility and risks upfront. Regulators and individuals expect organizations to act as a responsible steward for the data that is provided to them, and such organizations need to do more to live up to their promises and ensure responsible behavior, which can be achieved via an accountability-based approach.

In the following sections the relationship between these means for addressing privacy in the cloud is analysed. In this paper, the focus is on the way in which these categorisations relate and can be used in combination rather than the mechanisms and controls themselves (including encryption) that are used within them to help achieve privacy in the cloud. For an analysis of the latter, see for example [6,48], and the accountability tools being developed within the EU Cloud Accountability Project [14].

3 To What Extent Is Information Security an Integral Part of Privacy by Design?

First, the relationship between security and privacy is considered, before an analysis is provided about the role of information security in privacy by design.

3.1 The Relationship between Privacy and Security

At the broadest level (and particularly from a European standpoint), *privacy* is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights (1948) and subsequently in the European Convention on Human Rights and national constitutions and charters of rights. There are various forms of privacy, ranging from 'the right to be let alone' [15], 'control of information about ourselves' [16], 'the rights and obligations of individuals and organisations with respect to the collection, use, disclosure, and retention of personally identifiable information' [17], focus on the harms that arise from privacy violations [18] and contextual integrity [19].

For organisations, privacy entails the application of laws, policies, standards and processes by which personal information is managed. The fair information practices (FIP) developed in US in 1970s [20] and later adopted and declared as principles by the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe [21] form the basis for most data protection and privacy laws around the world. This framework can enable sharing of personal information across participating jurisdictions without the need for individual contracts. It imposes requirements on organisations including data collection, subject access rights and data flow restrictions. In Europe, the European Data Protection Directive 95/46/EC (and its supporting country legislation) implements these FIP principles, along with some additional requirements including transborder data flow restrictions. Other privacy-related restrictions may also be imposed (e.g. on cookie usage by the recent EU ePrivacy Directive). Legislation similar to the European Data Protection Directive has been, and continues to be, enacted in many other countries. In contrast, the US does not have a comprehensive regime of data protection but instead has a variety of sector-based or state level legislation and places few if any restrictions on transborder data flow. For further details, see [5].

Security mechanisms protect data by maintaining its confidentiality, integrity and availability; associated functionalities may also be provided, notably: authentication, access controls, data retention, storage, backup, incident response and recovery. Confidentiality is sometimes confused with privacy, but is “The property that information is not made available or disclosed to unauthorized individuals, entities or processes” [22].

Privacy differs from security, in that it relates to handling mechanisms for personal information, although security is one element of that. For example, the FIP can be broadly described as follows, where security is one of the principles:

1. *Data collection limitation:* data should be collected legally with the consent of the data subject where appropriate and should be limited to the data that is needed.
2. *Data quality:* data should be relevant and kept accurate.
3. *Purpose specification:* the purpose should be stated at time of data collection.
4. *Use limitation:* personal data should not be used for other purposes without the consent of the individual.
5. *Security:* personal data should be protected by a reasonable degree of security (i.e. safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data).
6. *Openness:* individuals should be able to find out what personal data is held and how it is used by an organisation.
7. *Individual participation:* an individual should be able to obtain details of all information about them held by a data controller and challenge it if incorrect.
8. *Accountability:* the data controller should be accountable for complying with these principles.

Legal requirements differ depending upon whether the organisation is a data controller and/or a data processor in a given situation:

- A *data controller* (DC) is an entity (which could be a person, public authority, agency or other body) which alone, jointly or in common with others determines the purposes for which and the manner in which any item of personal information is processed, and this is legally responsible for ensuring compliance requirements are met.
- A *data processor* (DP) is an entity which processes personal information on behalf and upon instructions of the data controller. Contractual agreements may add additional responsibilities or constraints with respect to privacy, although data protection laws stipulate that the organisation that is transferring personal information to a third party for processing remains responsible for the personal information.

The DC must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures need to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. If processing is carried out on behalf of a DC, the DC must choose a DP that provides sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures. A written contract or legal act is needed to bind the DP to the DC and should stipulate that the DP will act only on instructions from the DC [1].

Clarification of DC and DP responsibilities is key in cases where personal information is collected and used within cloud scenarios. The provider of cloud services can be a DP and/or a sole or joint DC. For analysis of how this is likely to change with respect to the forthcoming EU Regulation, see [23,24]. The proposed EU Regulation [2] increases the responsibility and accountability of DCs and DPs. The DC should implement appropriate procedures to ensure that the data processing carried out by the Cloud Service Provider (CSP) complies with the Regulation - but it is difficult for a business customer - especially a Small/Medium Enterprise (SME) - to influence the structure of cloud services, particularly for IaaS services. There can be multiple DPs in some scenarios (see [25] for example, which defines an accountability framework for mobile environments). Contracts and SLAs define respective responsibilities, but some of the responsibility cannot be transferred to the CSP, both in terms of security responsibilities and legal responsibilities.

Cloud providers may be constrained by the levels of security they can offer for different types of cloud. It may be difficult for a service provider to determine if the level offered is appropriate if it does not know what type of data may be stored in the cloud by the customer. Furthermore, security levels need to be enhanced to win business in certain industry sectors (e.g. financial services and health).

3.2 The Role of Security in Privacy by Design

Privacy by Design refers to the philosophy and approach of embedding privacy into design specifications [26-28]. It applies to products, services and business processes. The main elements are:

1. Recognition that privacy concerns must be addressed
2. Application of basic principles expressing universal spheres of privacy protection
3. Early mitigation of privacy concerns when developing information technologies and systems, across the entire information life cycle
4. Need for qualified privacy input; and
5. Adoption and integration of privacy-enhancing technologies (PETs).

In essence, companies should build in privacy protections at every stage in developing products, and these should include reasonable security for consumer data, limited collection and retention of that data, as well as reasonable procedures to promote data accuracy. Various companies have produced detailed privacy design guidelines [29] and methodologies about how to integrate privacy considerations and engineering into the development process [30]. The process can include building privacy into technical solutions by including privacy-enhancing features or through privacy solutions that manage the data from the code level up, as described further below.

'Privacy by policy' is the standard current means of protecting privacy rights through laws and organisational privacy policies, which must be enforced. Privacy by policy mechanisms focus on provision of notice, choice, security safeguards, access and accountability (via audits and privacy policy management technology). Often, mechanisms are required to obtain and record consent. The 'privacy by policy' approach is central to the current legislative approach, although there is another approach to privacy protection, which is 'privacy by architecture' [31], which relies on technology to provide anonymity. The latter is often viewed as too expensive or restrictive. Although in privacy by policy the elements can more easily be broken down, it is possible (and preferable) to enhance that approach to cover a hybrid approach with privacy by architecture.

Privacy settings are an important aspect of online privacy. *Privacy by default* is a software design concept that is presently being promoted by a number of data protection authorities, including the EC. Privacy by default would prohibit the collection, display, or sharing of any personal data without explicit consent from the customer. More detailed definitions often include the requirement that privacy settings that limit the sharing of personal data be turned on by default. Notable examples of this approach include MS Internet Explorer 6 and above, in which privacy settings blocked cookies, and also Internet Explorer 10, in which the default setting is that the Do Not Track (DNT) flag is set to "on". Privacy by default is not really a security issue, although there are good settings from a privacy point of view related to security aspects, e.g. restricting access to personal data via a 'deny by default' access control policy.

Privacy enhancing technologies (PETs) are solutions whose specific purpose is to help consumers and companies to protect their privacy [32]. These include those technologies that permit developers, solution providers and service companies to add privacy enhancements to their solutions. For example, PETs include anonymisers and pseudonymisers (e.g. anonymous Web and email access), history-clearing tools, pop-up blockers, anti spam, anti spyware, cookie managers, secure file deletion and software for firewalls.

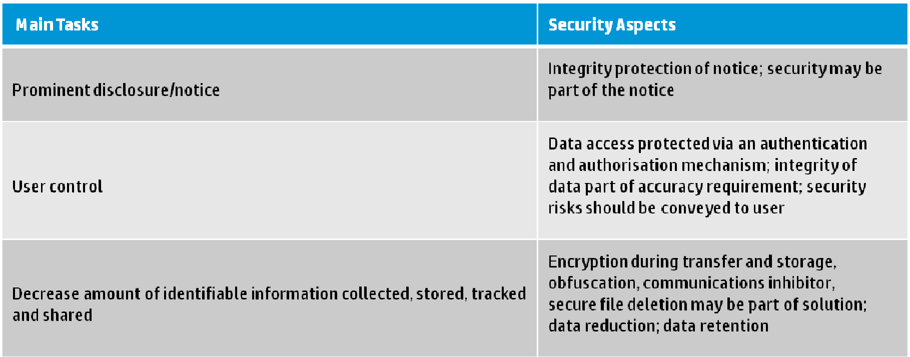
Privacy aware technologies (PATs) are standard non-privacy related solutions that include features that enable users to protect their privacy, e.g. passwords, file access security, communication inhibitor, encryption. The OECD privacy principles may be used to guide good system design, for example by addressing the following issues during the design process:

- *Collection limitation*: Investigate what data systems are collecting automatically; Determine what data you really need and collect only that
- *Data quality*: Keep data up to date; Use data for relevant purposes
- *Purpose specification*: Work out why you are collecting data and explain it in your policy

- *Use limitation*: Keep track of purpose for which data was collected; obtain consent for other uses; Mechanisms may be needed for obtaining and recording consent
- *Security safeguards*: If you collect it, you need to secure it
- *Openness*: Users need to be informed of all data collection, including implicit collection using cookies, behavioral tracking, etc.
- *Individual participation*: Work out how you are going to handle access, correction and purging of data
- *Accountability*: Be proactive about developing policies, procedures, and software to comply with these principles

Security aspects can be involved within privacy by design tasks, as illustrated in Table 2.

Table 2. Privacy by Design



Main Tasks	Security Aspects
Prominent disclosure/notice	Integrity protection of notice; security may be part of the notice
User control	Data access protected via an authentication and authorisation mechanism; integrity of data part of accuracy requirement; security risks should be conveyed to user
Decrease amount of identifiable information collected, stored, tracked and shared	Encryption during transfer and storage, obfuscation, communications inhibitor, secure file deletion may be part of solution; data reduction; data retention

There can be security aspects within several stages of the data lifecycle (Collection-Storage-Processing and Transfer-Archival-Destruction), including: secure storage, transfer, retention and disposal (inc. physical security, encryption); disclosure to authorised, authenticated parties; data protection plan of third parties, inc. confidentiality and security requirements in vendor management; data loss prevention; risk assessment; compliance and auditing; securing backup; disaster recovery. Security aspects may also be involved within different phases of the privacy design lifecycle:

- *Initiation*: setting high level recommendations
- *Planning*: Describing privacy requirements in detail
- *Execution*: Identifying problems with proposed privacy solutions; Considering alternatives; Documentation
- *Closure*: Audit; Change control; Considering privacy during backup; Fault repair; Business continuity; Disaster recovery, etc.
- *Decommission*: Ensuring secure deletion and disposal of personal data

In conclusion, from the above analysis it can be seen that information security is an integral part of privacy by design, although the latter includes a number of other considerations and techniques.

4 What Is the Relationship of Accountability to Privacy by Design?

First the notion of accountability is explained, and then its relationship to design for privacy and to external standards is considered. While regulatory frameworks involving accountability provide a foundation for data protection in the cloud, none are specifically designed with cloud computing in mind.

4.1 The Concept of Accountability

The concept of accountability is used in various different communities in a slightly different sense, and there is no commonly agreed definition. In particular, in data protection regulation since the 1980s, accountability has been used in the sense that the DC is responsible for complying with particular data protection legislation and, in most cases, is required to establish systems and processes which aim at ensuring such compliance. The Article 29 Data Protection Working Party [33], the European Data Protection Supervisor [23], as well as the data protection and privacy regulators at the 31st International Conference of Data Protection and Privacy Commissioners [34] have all recently paid special attention to the principle of accountability. In IT governance, accountability is used in the sense that the information security management system of an organisation is meant to generate assurance, transparency and responsibility in support of control and trust. For corporate governance, accountability is viewed as an organisational privacy management program. There are also other types of usage coming from social science and computer science. For example, the privacy-oriented definition of accountability given in ISO standard 29100 [35] expresses accountability in terms of the practices associated with it in organisations: *"Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organisation, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches."* For further discussion of the concept, see for example [36,37]. Overall, accountability can be thought of in terms of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly [38].

The scope of accountability can cover a range of diverse aspects, including politically sensitive areas such as intrusive Government surveillance and the responsibilities of organizations to contribute fairly to their local societies via appropriate payment of taxes. Some of these, like Sarbanes-Oxley requirements, do not have a strong connection to privacy. The issue of accountability in relation to intrusive governmental surveillance for national security purposes is more general than cloud computing, although two secret mass surveillance programmes recently revealed (ie. PRISM and Tempora) have a connection to cloud computing in that information collected by certain US-based cloud companies about EU citizens was made available to the US and UK security services. Accountability controls that centre on enforcement of private contracts and domestic data protection legislation would not provide effective protection against such activities; instead, the relevant sphere of governance is such cases seems to be in application of the principle of legality, proportionality and judicial and parliamentary accountability, potentially combined with technical measures to help make scrutiny of social media accountable [39]. Here we focus on the reduced scope of corporate accountability for handling personal data in the cloud, and use accountability in the following sense: *Accountability for an organisation consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, for processing, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly* [37, 38].

Accountability can be provided within an organisation, by means of the organisation identifying risks, having appropriate policies that mitigate risks, mechanisms for enforcement internally and for monitoring that these are effective within the enterprise, and for internal and external validation of this. In addition, provision of transparency and redress to customers and end users is also very important. Technology can be used for example to strengthen the enforcement and monitoring of policies, to support design for privacy to help provide assurance and transparency and enforce privacy obligations along the service provision chain.

These elements of risk assessment, transparency and redress are captured within the core elements of implementing an accountability project within an organisation specified within the Galway/Paris projects [43]. In terms of risk assessment, this involves on-going risk assessment and mitigation relating to new products or processes, as well as regular risk assessment and validation of the accountability programme itself. This analysis influenced the similar guidance for a privacy management programme provided by the Privacy Commissioners of Canada, Alberta and British Columbia [44], which again included privacy risk assessment mechanisms as well as on-going assessment and revision of the programme controls.

Risk assessment (a core security process) is particularly important for accountability because it is a central part of the process used to determine and demonstrate that the policies (whether reflected in corporate privacy and security policies or in contractual obligations) that are signed up to and implemented by the organisation (that is taking an accountability-based approach) are appropriate to the context. The type of procedures and mechanisms vary according to the risks represented by the processing and the nature of the data [4,40,41]. In the cloud context, as considered in section 2.2, the risks also depend upon the cloud service and deployment models used [4,6]. Further research to provide risk assessment mechanisms in relation to cloud service provision is being carried out within the Cloud Accountability Project [14].

Existing organisational risk assessment processes need to be enhanced to meet the requirements above, or else supplemented with separate privacy-specific risk assessment. Privacy impact assessments are already being rolled out as part of a process to encourage privacy by design [42]: in November 2007 the UK Information Commissioners Office (ICO) (an organisation responsible for regulating and enforcing access to and use of personal information), launched a Privacy Impact Assessment (PIA) [42] process (incorporating privacy by design) to help organisations assess the impact of their operations on personal privacy. This process assesses the privacy requirements of new and existing systems; it is primarily intended for use in public sector risk management, but is increasingly seen to be of value to private sector businesses that process personal data. Similar methodologies exist and can have legal status in Australia, Canada and the USA [42]. The methodology aims to combat the slow take-up to design in privacy protections from first principles at the enterprise level. Usage is increasingly being encouraged and even mandated in certain circumstances by regulators [42]. Data impact assessment may also become an obligation for some high risk contexts within the forthcoming EU regulation [cf. Article 33: 2].

4.2 The Relationship between Accountability and Design for Privacy

A major driver for an accountability-based approach is to provide an incentive for organizations to 'do the right thing', in terms of decreasing regulatory complexity, easing transborder data flow restrictions while avoiding increased privacy harm, encouraging best practice and using strong punishment as a deterrent. For example, in response to the seemingly insufficient reflection of EU data protection principles and obligations in concrete measures and practices used by organisations, the Article 29 Working Party advocated in its Opinion on the principle of accountability [33] that such a general principle could help move data protection 'from theory to practice', as well as provide a means for assisting data protection authorities in their supervision and assessment tasks. Organisations are allowed increased control over aspects of compliance (i.e. which tools and mechanisms to use in order to achieve compliance), but at the expense of having to demonstrate on an ongoing basis that these mechanisms are appropriate for their business context, and operationally work as expected. For example, the Article 29 Working Party extended a similar notion of accountability to that contained within the OECD guidelines (as considered above in Section 3) with a requirement for DCs to be able to demonstrate compliance to supervisory authorities upon request [33]. Although some specific measures would have to be implemented for most processing operations, for reasons of scalability and flexibility, the suitability of measures needs to be determined on a case-by-case basis, with particular reference to the type of data and to the risks involved.

It is important to state that accountability should not be seen as an alternative to privacy [45]. Instead, as shown in Figure 3, accountability and privacy by design are complementary, in that the latter provides mechanisms and controls that allow implementation of principles and standards, whereas accountability makes organizations responsible for providing an appropriate implementation for their business context, and addresses what happens in case of failure (i.e. if the account is not provided, is not adequate, if the organisation's obligations are not met e.g. there is a data breach, etc.). Privacy by Design may to some extent incorporate corporate accountability mechanisms [46], in that a privacy management program can be seen as bridging between accountability and privacy by design.

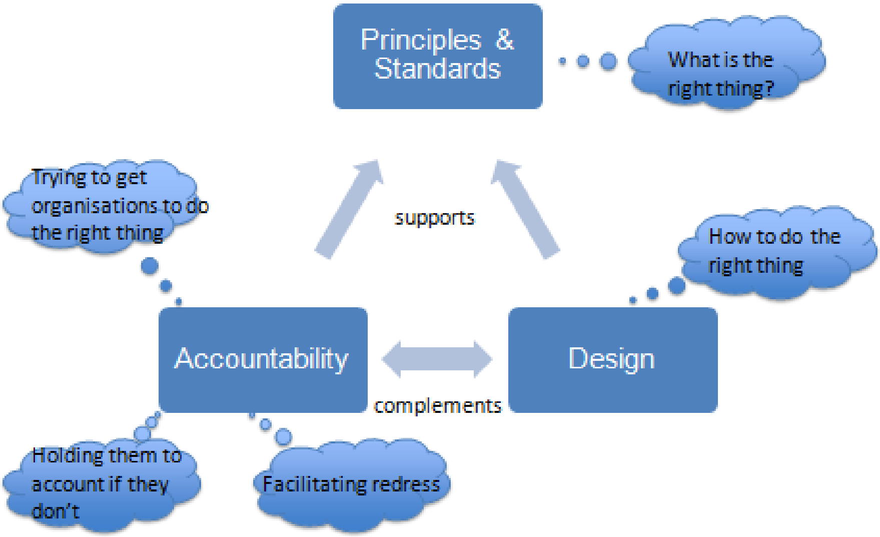

Principles & Standards
What is the right thing?
Trying to get organisations to do the right thing
supports
How to do the right thing
Accountability
Design
complements
Holding them to account if they don't
Facilitating redress

Fig. 3. Accountability Context

At the top of Figure 3, standards are external criteria against which the organization needs to measure themselves and demonstrate compliance against where relevant to the business context. Some of these are technical best practice standard, as considered further within the following section. Others are social principles that are reflected in legislation, such as the OECD privacy principles discussed in section 3. Accountability should underpin the principles and standards set by society rather than undermining them; such principles should be subject to change via a democratic process. Additional constraints may come from other legal and stakeholder requirements. Together, these set societal, regulatory and contractual obligations that organizations need to meet, and for which they are accountable to certain other parties, such as business partners and regulators.

In Section 3 it has been considered how these principles may be reflected in privacy by design, via PATs and PETs. There are a range of different privacy and security controls that could be used, including encryption, that suit different contexts (see for example [47,48]). Implementation and configuration choices also need to be decided upon.

Accountability is concerned with governance mechanisms related to punishment, remediation, transparency, providing a trustworthy account, holding to account, data breach detection and notification, etc. Correspondingly, accountability mechanisms and tools do not focus on providing privacy and security tools *per se*, but rather on formation of appropriate organizational policies, detection of violation of obligations, notification, remediation in complex environments, increased transparency without compromising privacy, provision of a trustworthy account, improved verification and assurance, etc. Accountability should involve checking and proving that data stewardship is in place along the service provision chain, which involves showing that appropriate privacy and security 'design' controls are being used. Hence, accountability should not be a replacement for certain other procedures, including privacy controls, but should be used to complement these [42] and an accountability-based approach should not be used to justify the abandonment of privacy rights and principles.

Although organisations can select from accountability mechanisms tools in order to meet their context, the choice of such tools needs to be justified to external parties. It would be a mistake to have this reliant upon self-certification or weak certification processes. As Bennett points out [p45: 45], due to resource issues regulators will need to rely upon surrogates, including private sector agents, to be agents of accountability, and it is important within this process that they are able to have a strong influence over the acceptability of different third party accountability mechanisms. This can be achieved via independent testing of practices, provision of evidence that is taken into account, including auditing against the ISO 27001 series and associated cloud security standards.

4.3 The Role of Standards

From the definition of accountability given above, it can be seen that standards and best practice are a reference point when organizational policies are formed as part of an accountability-based approach, and the latter (and the internal organizational practices) need to be justified against those. This extends also across to justification of the selection and usage of appropriate cloud service providers with appropriate controls in place.

Examples of such standards in the cloud space include organisational security guidance for the cloud [4,5], guidance to UK organisations on the use of cloud computing [49] and higher-level enterprise risk management guidelines for executives to enable them to identify, monitor, and mitigate or accept the risks that come with using cloud computing [50].

In addition, competing architectural standards are being developed, with big cloud vendors pushing their own mutually incompatible *de facto* standards. Limitations include: differences between common hypervisors; gaps in standard APIs for management functions; lack of commonly agreed data formats; issues with machine-to-machine interoperability of web services. The lack of standards makes it difficult to establish security frameworks for heterogeneous environments and forces people for the moment to rely on common security best practice. As there is no standardised communication between and within cloud providers and no standardized data export format, it is difficult to migrate from one cloud provider to another or bring back data and process it in-house.

The EC is driving a number of initiatives around harmonization across the member states for cloud. These reflect concerns about trust in cloud computing and include standards and mechanisms for interoperability and data portability, security, cloud and compliance. New requirements are coming through for cloud providers, e.g. with regard to breach notification and cyber incident notification, penalties are increasing, and business environments are getting more complex. The draft data protection legislation [2] has already been discussed above. In addition, Neelie Kroes (the Vice-President of the European Commission responsible for the Digital Agenda) has launched a *European Cloud Computing Strategy* aiming at

- more clarity and knowledge about the applicable legal framework (includes development of model contracts & BCRs)
- making it easier to verify compliance with the legal framework (e.g. through standards and certification)
- developing it further (e.g. through a European Cloud Partnership to drive innovation and growth from the public sector).

A Key Action within this cloud strategy is to cut through the jungle of standards, in particular building upon NIST standardisation, ongoing work within the ETSI cloud group and ENISA/CSA voluntary cloud certification schemes.

In February 2013 the European Commission published a *cybersecurity strategy* alongside a *draft directive on network and information security*. Once implemented, cloud service providers and many others will all be covered by a range of data security obligations including adopting risk management practices and reporting major security incidents. The EC expects the directive to be adopted in 2015. As part of this strategy, the EC will set up in June this year a platform on network and information security bringing together relevant public and private stakeholders, to identify good cybersecurity practices across the value chain and create favourable market conditions for development and adoption of secure IT solutions.

In summary, the relationship between accountability and privacy by design is both complementary and at times closely interlinked, such as when privacy impact assessment is deployed as a key part of organizational privacy management programmes.

5 Conclusions

There is a complex and interesting relationship between privacy, security and accountability. For example, privacy relates to personal information only, whereas security and confidentiality can relate to all information, but consideration of the security of personal information is an essential aspect within the process of privacy by design. Accountability has a broader scope than privacy but is often used specifically in the context of privacy governance. In this sense, accountability can be viewed as being complementary to privacy by design, in that it can help support the implementation of privacy principles within organisations.

Cloud computing creates new dynamics to such analysis in that there is an additional role of cloud provider, and indeed there could be several such parties. Top barriers in providing cloud computing services include lack of customer trust and regulatory complexity in global business environments: cloud consumers want data processors to respect their obligations and policies and be compliant (especially as they may be legally liable). A combination of privacy by design and accountability can help provide solutions to such issues.

Further work on development of such solutions is being carried out within the Cloud Accountability project [14], which is an integrated research project under the EU Framework 7 programme addressing data governance problems and developing accountability solutions for the cloud.

Acknowledgements. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 317550. Thanks also to Simon Shiu who provided me with a version of Figure 1 and some associated insights, as well as colleagues within the A4Cloud project for feedback on related materials.

References

1. European Commission (EC): Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)
2. European Commission: Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (January 2012)
3. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (September 2011)
4. Catteddu, D., Hogben, G. (eds.): Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report (November 2009)
5. Cloud Security Alliance (CSA): Security Guidance for Critical Area of Cloud Computing V3.0 (2011)
6. Pearson, S.: Privacy, Security and Trust in Cloud Computing. In: Pearson, S., Yee, G. (eds.) Privacy and Security for Cloud Computing, Computer Communications and Networks. Springer (2012)
7. European DG of Justice: Article 29 Working Party, Opinion 05/12 on Cloud Computing (2012)
8. Baldwin, A., Pym, D., Shiu, S.: Enterprise Information Risk Management: Dealing with Cloud Computing. In: Pearson, S., Yee, G. (eds.) Privacy and Security for Cloud Computing, Computer Communications and Networks. Springer (2012)
9. CSA: The Notorious Nine Cloud Computing Top Threats in 2013. Top Threats Working Group (2013)
10. Ko, R.K.L., Lee, S.S.G., Rajan, V.: Understanding Cloud Failures. IEEE Spectrum 49(12), 84 (2012)
11. Jansen, W., Grance, T.: Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144, NIST (December 2011)
12. Liu, F., et al.: NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292 (September 2011)
13. CSA: Cloud Controls Matrix, v1.4, `https://cloudsecurityalliance.org/research/ccm/`
14. Cloud Accountability Project (A4Cloud), `http://www.a4cloud.eu`
15. Warren, S., Brandeis, L.: The Right to Privacy. 4 Harvard Law Review 193 (1890)

16. Westin, A.: Privacy and Freedom. Atheneum, New York (1967)
17. American Institute of Certified Public Accountants (AICPA) and CICA: Generally Accepted Privacy Principles (August 2009)
18. Solove, D.J.: A Taxonomy of Privacy. University of Pennyslavania Law Review 154(3), 477 (2006)
19. Nissenbaum, H.: Privacy as Contextual Integrity. Washington Law Review, 101–139 (2004)
20. Privacy Protection Study Commission: Personal Privacy in an Information Society, United Statues Privacy Protection Study Commission Fair Information Practices (1977)
21. Organisation for Economic Co-operation and Development (OECD): Guidelines for the Protection of Personal Data and Transborder Data Flows (1980)
22. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements (2005)
23. EDPS: Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe" (2012)
24. EDPS: Responsibility in the Cloud should not be up in the air". Article EDPS/12/15 (2012), `http://europa.eu/rapid/press-release_EDPS-12-15_en.htm`
25. GSMA Mobile and Privacy: Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development (February 2012)
26. Cavoukian, A.: Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In: Yee, G. (ed.) Privacy Protection Measures andTechnologies in Business Organisations: Aspects and Standards, pp. 170–208. IGI Global (2012)
27. UK Information Commissioners Office (ICO): Privacy by Design. Report (2008)
28. Federal Trade Commission (FTC): Protecting Consumer Privacy in an Age of Rapid Change: Recommendations for Business and PolicyMakers. FTC Report (March 2012)
29. Microsoft Corporation: Privacy Guidelines for Developing Software Products and Services, Version 2.1a (2007)
30. Cannon, J.C.: Privacy: What Developers and IT Professionals Should Know. Addison Wesley (2004)
31. Spiekermann, S., Cranor, L.F.: Engineering Privacy. IEEE Transactions on Software Engineering 35(1), 67–82 (2009)
32. Shen, Y., Pearson, S.: Privacy Enhancing Technologies: A Review. HP Labs External Technical Report, HPL-2011-113 (June 2011)
33. European DG of Justice: Article 29 Working Party. Opinion 3/2010 on the principle of accountability (WP 173) (July 2010)
34. ICDPP: 31st International Conference of Data Protection and Privacy 'Data protection authorities from over 50 countries approve the "Madrid Resolution" on international privacy standards' (2009), `http://www.gov.im/lib/docs/odps//madridresolutionpressreleasenov0.pdf`
35. ISO/IEC 29100: Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27
36. Papanikolaou, N., Pearson, S.: A Cross-Disciplinary Review of the Concept of Accountability. In: Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC) (May 2013)
37. Pearson, S., Charlesworth, A.: Accountability as a Way Forward for Privacy Protection in the Cloud. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) Cloud Computing. LNCS, vol. 5931, pp. 131–144. Springer, Heidelberg (2009)

38. Catteddu, D., et al.: Towards a Model of Accountability for Cloud Computing Services. In: Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC) (May 2013)
39. Omand, D., Bartlett, J., Miller, C.: DEMOS Report (2012), http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327
40. CNIL: Methodology for Privacy Risk Management (2012), http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
41. Castelluccia, C., Druschel, P., Hübner, S., et al.: Privacy, Accountability and Trust - Challenges and Opportunities. ENISA (2011)
42. Tancock, D., Pearson, S., Charlesworth, A.: Analysis of Privacy Impact Assessments within Major Jurisdictions. In: Proc. PST 2010, Ottawa, Canada. IEEE (August 2010)
43. Center for Information Policy Leadership (CIPL): Demonstrating and Measuring Accountability: A Discussion Document. Accountability Phase II –The Paris Project (2010)
44. Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia: Getting Accountability Right with a Privacy Management Program (April 2012)
45. Bennett, C.J.: The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: Guagnin, D., et al. (eds.) Managing Privacy through Accountability, pp. 33–48. MacMillan (2012)
46. Cavoukian, A., Taylor, S., Abrams, M.: Privacy by Design: Essential for Organisational Accountability and Strong Business Practices. Identity in the Information Society 3(2), 405–413 (2010)
47. Camenisch, J., Fischer-Hubner, S., Rannenberg, K. (eds.): Privacy and Identity Management for Life. Springer (2011)
48. Mowbray, M., Pearson, S.: Protecting Personal Information in Cloud Computing. In: Meersman, R., et al. (eds.) OTM 2012, Part II. LNCS, vol. 7566, pp. 475–491. Springer, Heidelberg (2012)
49. Information Commissioner's Office (ICO): Guidance on the Use of Cloud Computing (2012)
50. Horwath, C.: Enterprise Risk Management for Cloud Computing, COSO (June 2012)