Enhancing Accountability in the Cloud

Martin Gilje Jaatun[a,*], Siani Pearson[b], Frédéric Gittler[b], Ronald Leenes[c], Maartje Niezen[c]

[a] *SINTEF ICT, NO-7465 Trondheim, Norway*
[b] *HP Labs, Bristol, UK*
[c] *Tilburg University, The Netherlands*

Abstract

This article focuses on the role of accountability within information management, particularly in cloud computing contexts. Key to this notion is that an accountable Cloud Provider must demonstrate both willingness and capacity for being a responsible steward of other people's data. More generally, the notion of accountability is defined as it applies to the cloud, and a conceptual model is presented related to the provision of accountability of cloud services. This allows a consideration of accountability at various different levels of abstraction, including the operationalisation of accountability. It is underpinned by fundamental requirements for strong accountability, which in particular are aimed at avoiding risks in the provision and verification of accounts (that include different types of accountability evidence and notifications, that may need to be provided to other cloud actors including data subjects, cloud customers and regulators). In addition, the article sketches what kind of tools, mechanisms and guidelines support this in practice, and discusses these in the light of the upcoming European Data Protection Regulation.

Keywords: Cloud computing, accountability, security, privacy

*Corresponding author

1. Introduction

Accountability in the online / Internet sector came into play when solutions were sought for governing the more complicated, networked and global environment for international data transmissions. With cloud computing, this environment has become even more complex, networked and global: cloud computing (often) involves multiple chains of stakeholders and services, offers many more services than traditional information technologies have been able to offer thus far, and with greater flexibility. The governance of this environment, in legislative terms, has changed focus from defining the legal regime to investigating how data is actually protected by real organisations in receiving jurisdictions (Bennett, 2012). At a European level this trend is confirmed by the General Data Protection Regulation (GDPR)[1] that aims to reform data protection rules in the EU in order to: meet challenges resulting from globalisation and the use of new technologies, strengthen individuals' rights while ensuring a free flow of personal data, and provide a coherent data protection framework to support effective implementation (European Commission, 2012). In other words, the focus is expanded from adequacy assessments to "how to govern accountable behaviour with respect to sensitive data and personal information". The legal regime thus explicitly delegates responsibility to the cloud sector requiring other forms of governance. Cloud providers are no longer accountable for their own business only, they have to demonstrate their willingness and capacity in handling people's information (be it personal or sensitive data) responsibly. Yet, being a responsible steward of other people's information is easier said than done. The Accountability for Cloud (A4Cloud) project has studied the notion of accountability and its introduction in cloud ecosystems and cloud providers' practices. This paper outlines the fundamental requirements that must be met by accountable organisations, and sketches what kind of tools, mechanisms and guidelines support the introduction of 'accountability' in daily practice of the online sector, specifically the cloud ecosystem.

Key features of the cloud are the offering of generic services and its

[1]The GDPR, COM(2102) 11 final, of 25-01-2012, was discussed under trilogue by the European Commission, European Parliament, and European Council, resulting in a commonly agreed version in December 2015 that will be formally adopted by the European Parliament and Council in the beginning of 2016. The new rules will become applicable two years thereafter.

ubiquity (Mell and Grance, 2011). The offering of generic services sets Cloud Providers apart from many traditional service providers. Depending on the offered service model, there are specific boundaries of concern: an Infrastructure-as-a-Service (IaaS) provider will generally see the customer's data as a bag of bits, whereas a Software-as-a-Service (SaaS) provider sees structured data which more readily can be identified as information. Moreover, Cloud Providers offer services all over the world with little restrictions enforced by (inter)national boundaries.

The inherent ubiquitous nature of the Cloud introduces a more complicated, networked and global environment for international data transmissions. Cloud customers have come to expect services available anytime, from anywhere. For Infrastructure as a Service (IaaS), for instance, interoperability is an important factor; users want to be able to migrate payloads both within a given provider and between providers. This implies that the offered service should not be specific to any one provider, nor to any single customer. However, thus far a standard framework is lacking, leading to problems such as vendor-lock in and complicating the ease of use.

The Cloud has been used for many non-critical purposes by both individuals and enterprises for some time, but users (and particularly, potential users) of cloud services are currently not convinced by the balance of risk against opportunity (see Table 1 for a brief summary of some Cloud-specific features and associated privacy and security challenges, as identified by Pearson (2013)). In general, security concerns are often cited as the most prominent reason for not using cloud computing (Rong et al., 2013), and a recent UK survey found that 90 % of large organisations and 74 % of small businesses have suffered a security breach in the last year (Miller et al., 2015). A recent UK case study illustrates, however, that security risks introduced by deployment of cloud computing can be related to how it is used, rather than to any intrinsic properties of cloud computing as a technology (Jones, 2015). At the same time, customers of cloud users, especially end-users, frequently do not understand the need to control access to personal information (Jaatun et al., 2012). This is particularly evident in the context of social media, where the users are not the customers, but the product (being sold to marketers). On the other hand, some users might understand the risks, and yet have inadequate means to address them (Cattaneo et al., 2012). In order to make the Cloud a viable alternative for applications with more stringent security and privacy requirements such as those involving sensitive personal data (e.g., medical or health related data), accountability of the service providers is key

(Jaatun et al., 2014). In fact, the inclusion of 'accountability' as an asset in the market system of cloud computing aims to ensure increased attention to 'customer driven' services, and it balances the lack of customers' possibility to choose other cloud services (e.g., due to vendor lock-in or the inherent nature of cloud to offer generic services).

Table 1: Cloud Computing Features and Related Issues (Pearson, 2013)

Cloud feature	**Related privacy and security issue**
Multi-tenancy	Data of co-tenants may be revealed in an investigation of another tenant, isolation failure, improper deletion of data
Complex, dynamically changing environment and data flows	Ensuring appropriate data protection, overlapping responsibilities, unauthorized secondary usage of data, vendor demise, lack of transparency
Data duplication and proliferation; unknown geographical location	Exacerbation of trans-border data flow compliance issues, detecting and determining who is at fault if privacy breaches occur
Convenient and enhanced data access from multiple locations	Data access from remote geographic locations subject to different legislative regimes, subpoenas, access by foreign governments; employees may unilaterally decide to use Cloud services for enterprise purposes without due regard to organizational policies or risk assessment

In the context of protecting data stored and transferred in service provisioning chains, Cloud Providers have to demonstrate their willingness and capacity in handling people's information, be it personal or sensitive data, responsibly throughout the chain of service providers involved in delivering a service to an end-user. This paper will build on the accountability notion as defined in the Galway project (CIPL, 2009) and makes use of existing studies in public administration (Bovens, 2007; Hood, 2010) and work on the right to control one's personal data (Westin, 1967).

To hold cloud (and other) service providers accountable for how they deliver services and how they manage personal, sensitive and confidential information in the cloud, there is a need for an orchestrated set of mechanisms: preventive (mitigating risk), detective (monitoring and identifying risk and policy violation), and corrective (managing incidents and providing redress) (Pearson et al., 2012). Suppliers within cloud eco-systems need to be able to differentiate themselves in what ultimately is a commodity market. Being able to offer accountability as part of the service provision may represent a competitive edge for service providers catering to discerning cloud customers. In any case concerns regarding privacy, security, and data protection are a key obstacle that hinder the cloud industry to realize its full economic and technological potential (Catteddu and Hogben, 2009). This will also be tantamount to extending the cloud market, expanding the definition of "what it is possible to do in the Cloud".

Cloud-based storage of data that requires privacy assurance is typically deployed in private clouds. Heterogeneous cloud infrastructures make it difficult to have effective controls to check privacy compliance (often offered as an optional extra) in an automated way and the end-user has no means to verify that his/her privacy requirements are being fulfilled. Effective and profitable utilization of cloud services relies on data transfer and storage across services and different cloud infrastructures (which may have different jurisdictional restrictions). Furthermore, end user agreements are stated in natural languages, making it hard for computer programs to assess whether application providers respect data usage agreements.

Existing technologies filter information in different ways, including privacy-enhanced access control (Ardagna et al., 2010), Data Loss Prevention techniques[2], redaction (Bier et al., 2009), various privacy enhancing technologies and database proxies like Informatica's dynamic data masking tool (Informatica, 2013). Existing auditing frameworks typically manually verify the adequacy of the data handling controls used (American Institute of Certified Public Accountants, 2016; ISO, 2013). These procedures are extremely costly. Automated assurance is necessary to quickly evaluate the evidence that obligations with respect to personal data handling and business compliance requirements are being carried out (for instance, the collection of events showing who created a piece of data, who modified it and how, and so on).

[2]http://datalossprevention.com/

Governance, Risk management and Compliance (GRC) frameworks (e.g., RSA eGRC (EMS Corporation, 2016)) are a common means of automating compliance in enterprises but do not provide much breadth or strong co-design of technical and legal mechanisms and although they can target specific regulations, they rarely deal with concepts like privacy and transparency, with the notable exception of recent work within CSA[3].

This paper will first address the notion of accountability as it underlies a new conceptual framework and tools for emerging services within the cloud and future Internet services. Next, we briefly describe recent results on cloud customers willingness to pay for accountable services. In section 4 we then discuss the four main objectives that drive the research within the A4Cloud project. In order to attain these four objectives it is of importance to define the fundamental requirements that must be met by accountable organisations, which we outline in section 5. In section 6 we describe a conceptual accountability model that allows alignment of the tools and mechanisms with the descriptive and normative requirements of accountable organisations. An outline of various (possible) tools that fit both the accountability model and meet the objectives as set is given in section 7. The discussion in section 8 describes the context of the accountability model and reflects upon its feasibility to increase accountable behaviour of cloud service providers in the near future taking into account current developments on the international Cloud market and in legal frameworks.

2. Accountability notion

The concept of accountability in itself pre-dates the computing industry; Webster's 1828 dictionary (Webster, 1828) provides the following definition:

> ACCOUNTABIL'ITY, noun
>
> 1. The state of being liable to answer for one's conduct; liability to give account, and to receive reward or punishment for actions.
> 2. Liability to the payment of money or of damages; responsibility for a trust.

[3]https://cloudsecurityalliance.org/research/grc-stack/

The generic accountability notion has been contextualised for particular domains, such as public policy, the financial sector or enterprise operations. This is due to the characteristics of the specific contexts and the potential effectiveness of the concept in achieving 'good governance'. In the public sector, where government, for instance, is accountable to parliament in many democracies, financial punishment for malconduct might well be fairly ineffective as an element of accountability, whereas (stiff) financial fines might be effective in the financial sector. As a result of the context specificity of accountability, no universal definition of accountability exists. For enterprise operations, including IT, we are proposing to define accountability as being the state of accepting allocated responsibilities, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly; responsibilities being derived from law, social norms, agreements, organizational values and ethical obligations.

Within the context of data protection and privacy, the Galway project (CIPL, 2009) is notable. Despite the fact that Lampson (2004) already coined accountability more than ten years ago as one of the three core objectives of having a security policy, alongside usage control and availability, it remained a fairly abstract notion. The Galway project, led by the Centre for Information Policy Leadership, and consisting of a group of international experts from regulators, industry and academia, took significant steps to develop an accountability-based system. The Galway project (CIPL, 2009) defines an accountability-based approach to data protection to require:

> [...] that organisations that collect, process or otherwise use personal information take responsibility for its protection and appropriate use beyond mere legal requirements, and that they be accountable for any misuse of the information that is in their care.

Within the A4Cloud project, we have adopted the Galway approach and further particularised the notion of accountability to the Cloud context. In this context, accountability for an organisation (i.e., a cloud service provider) consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly. Our

concept of accountability is placed in the context of privacy and security and perceives accountability form the perspective of the user of cloud services, in the sense that they[4] have control over their data or the data entrusted to them by their users and which resides in the cloud.

Our notion of accountability takes the Galway perspective as a starting point and furthermore builds on theory and practice in public administration (Mulgan, 2000; Bovens, 2007; Hood, 2010) and privacy as the right to control one's personal data (Westin, 1967). Accountability, following the cited literature, is considered not to be a state, but rather a learning process in which organizations mature with respect to good governance. In our view the notion of accountability is not only descriptive ("accountability of some agent to some other agent for some state of affairs"), but also has a strong normative claim ("the promise of fair and equitable governance") that requires interaction between the two agents to establish the norms and reflect upon what responsible behaviour is, in line with scholarship and practice in public administration.

We move beyond the Galway model in elaborating what being accountable entails, focusing particularly on the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly. This clarification is possible since the consensus of what it means for a responsible organisation to protect personal data and to respect the individual's privacy has grown since the Galway project (Bennett, 2012; Charlesworth and Pearson, 2013).

In the A4Cloud project we have developed the notion of accountability for the Cloud computing context into an extensive conceptual framework on which various tools, mechanisms and guidelines that support accountable behaviour with data in daily practice in Cloud ecosystems are based. Before discussing the conceptual framework and its associated toolbox, we first outline the project's objectives to place the framework into context.

3. Public Willingness to Pay for Accountability in the Cloud

[4] "They" can refer to business users (that may offer services to their clients), or individuals that use cloud services for their own affairs.

[5] Costs indicated here are costs per year. A minus in front of the WTP means that people would want to pay less for a service if that attribute was present when compared to the baseline level.

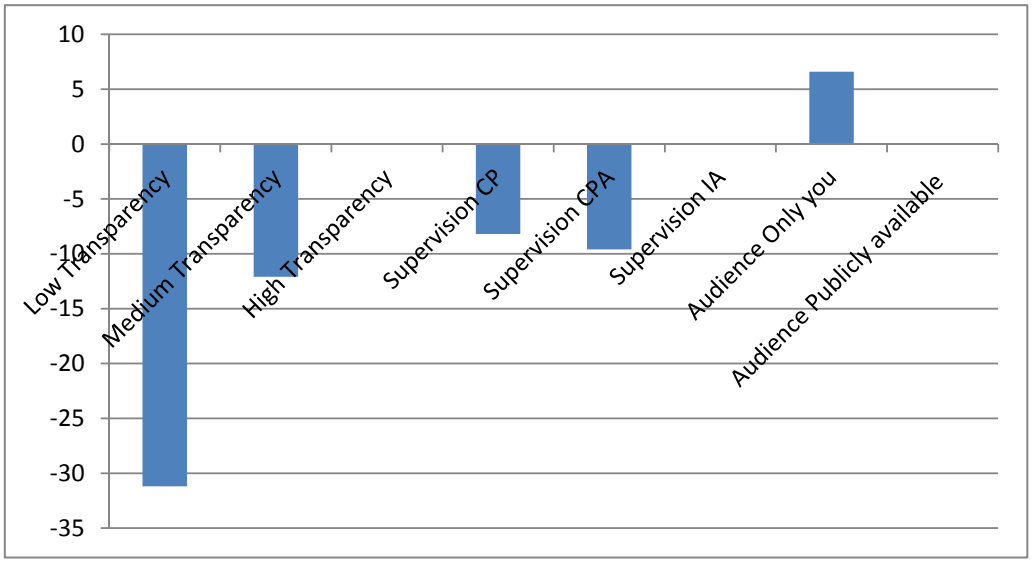

Figure 1: Willingness to pay for accountability[5]

An A4Cloud study on the individual end-users' willingness to pay (WTP) for accountability (Steijn and Niezen, 2015), i.e., in the form of a transparency tool, has demonstrated that end-users want to pay for insight about their (personal) data in the cloud and its use by cloud providers and possible others, yet cost is the most important factor influencing their decision to acquire an accountability tool or not, compared to the other attributes; level of transparency, offered supervision and audience of the offered information. A Choice-based Conjoint experiment demonstrated a general WTP of €31,20 per year for such a transparent cloud service (see Figure 1). However, for that particular amount respondents do expect to receive high transparency information rather than low. This high level of transparency information was also not to be disclosed to other (potential) service users (WTP €6,60/year). Moreover, the reliability of the information should be warranted via supervision by an independent authority (WTP €8,20/year). Cloud service providers or an association of such providers were less trusted to supervise the transparency process.

The latter is backed up by economic modeling of accountable cloud ecosystems. According to Prüfer, the best governance of a cloud ecosystem from an economic perspective is facilitated via so-called private ordering or self-governance. Independent private certification agencies are best equipped to

quickly and credibly reach consumers (private and business users) informing them about CSPs' accountability levels and also ruin defectors' reputations (Prüfer, 2013). Prüfer notes that SMEs that highly value accountability will be willing to pay more for certified and hence accountable CSPs than SMEs that value accountability less. It is this threshold that is important to keep in mind when developing accountability tools (Prüfer, 2013).

4. Objectives

For the purposes of this paper, accountability is to be understood in the context of protecting data stored and transferred in service provision chains, specifically related to cloud services. Although the initial focus is on data protection and hence on personal data[6], we believe that many of the principles and concepts equally can be applied in a business context in which 'confidential' business data is being handled. As such, we will extend beyond scenarios involving personal data, also taking into account situations in which there is an obligation to some person to keep other information confidential. Additionally, we maintain that accountability is poised to fill certain gaps that current Cloud privacy mechanisms and recommendations leave unanswered.

Based on the discussion above, we have derived the following objectives for our work in the A4Cloud project:

Objective 1 – facilitate choice: create tools that enable cloud end users to make choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.

Objective 2 – control and transparency: develop tools that enable cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers.

Objective 3 – compliance: develop tools to monitor and check compliance with users' expectations, business policies and regulations.

[6]At least in the European context in which the project is situated.

Objective 4 – recommendations and guidelines: develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.

5. Requirements

In the context of data protection, the starting point is that an accountable organisation must commit to responsible stewardship of other people's data. More specifically, the organisation should follow the accountability practices outlined in our conceptual model (see section 6), which in brief entail that it:

- defines what it does,
- performs what it defined,
- monitors how it acts,
- remedies any discrepancies between the definition of what should occur (norms) and what is actually occurring (behaviour),
- explains and justifies any action.

Basically the first four bullets describe the standard cybernetic loop (define, monitor, correct) (Wiener, 1948)[7] as well as the preventive, detective and corrective mechanisms discussed above. This also aligns well with the outcomes of the CIPL Galway (CIPL, 2009) and Paris (CIPL, 2010) projects.

These elements can be elaborated as follows.

1. **An accountable organisation must demonstrate willingness and capacity to be responsible and answerable for its data practices.**
   Data practices refer to the processing and storing of data; this primarily concerns personal data as defined in the Data Protection Directive 95/46/EC (European Parliament, 1995), but may extend to types of confidential information that do not involve personal data.

[7] Or the plan, do, check, and act components of Deming's circle of continuous improvement (Dybå et al., 2004).

2. **An accountable organisation must define policies regarding their data practices.**
   Policy is a shorthand for the wide variety of things that need to be defined by an accountable organisation. Policies (or norms) may take the form of written text (such as privacy statements or manuals), machine readable policies in a formal language or any form that conveys information about the way the organisation deals with the information within scope. Aspects of the data practices that need to be defined (may) include:
   - the entities involved in the processing of data and their responsibilities
   - the scope and context of processing data
   - the purposes and means of processing
   - data handling and data access policies
   - risk monitoring and risk mitigation
   - relevant external legal obligations (such as what legal obligations the organisation has in disclosing data to third parties (e.g., in the context of law enforcement)

   These items include information obligations as defined in the data protection legal framework and be based on business considerations related to the service provider's services, but extend those to include all elements that are relevant for customers to make informed choices about the organisation's service offering (from a privacy & data protection point of view) and that allow checking compliance later on (in the monitoring stage). Policies hence have external (e.g., the law, social norms) and internal (business objectives) sources that are relevant for the given context.
3. **An accountable organisation must perform what it promises.**
   The Cloud provider should develop its processes in line with the policies defined earlier to make sure that its behaviour is in accordance with these policies. This provides ex-ante certainty that policies are observed in actual operations.
4. **An accountable organisation must monitor its data practices.**
   An accountable organisation outlines how it processes data (policies), processes in accordance with these policies and has to be able to prove

(ex-post) that it acted according to their policies and hence has to monitor the actual data practices and keep records of the monitoring and its results (i.e., a running account).

5. **An accountable organisation must correct policy violations.**
   If discrepancies between the stated policies and actual (system) behaviour are detected, several things need to be done. First of all, the casue(s) of the violation need to be addressed, starting with stopping/preventing further violations ('stop the bleeding', for instance in the case of a data breach due to insecure passwords, preventing further breaches by (temporarily) preventing log-ins). Errors need to be corrected, and incidents need to be handled. This requires going back to the causes of the violation. If the violation is the result of a faulty process, the process needs to be repaired, or improved. If the violation results from a data breach or (other) cybercrime, the security needs to be improved, etc. Second the effects of the violation need to be addressed. This may, for instance, require data to be restored from back-ups in case of data loss, replacing account credentials in case of data breaches, recalling data from third parties that have unjustly received the data, or damages may need to be compensated (financially or otherwise) to those affected. In some cases, the effects are very difficult, or even impossible, to mitigate (e.g., data losses in transit). Third, the appropriate stakeholders need to be informed. In some cases the authorities (such as the Data Protection Authorities) need to be informed; in other cases the customer or affected data subjects may need to be informed (depending on, for instance, the policies as defined by the organisation).
6. **An accountable organisation must demonstrate policy compliance.**
   The final element of the accountability loop is demonstration of compliance with the adopted policies. An accountable organisation should be willing and able to demonstrate their policies, actual behaviour, and compliance with their policies and not only report policy violations. Furthermore it should show compliance in a timely fashion "reactively" (i.e., when prompted by the customer or regulator) and where possible "proactively" (proactive demonstration can in turn range from regular audits to continuous attestation). Furthermore, it should be able to demonstrate that the controls that are selected and used within the service provision chain are appropriate for the context and provide ev-

idence that the operational environment is satisfying the policies (cf. point 4 above).

In addition to the above, there is a need for accountability across the cloud service provision and governance chains, and not just in isolation for organizational cloud consumers or cloud service providers. Hence there is a need for provision of evidence of satisfaction of obligations right along the service provision chain, as well as aspects such as checking that chain partners are accountable too and that there has been proper allocation of responsibilities along the service provision chain. These requirements need to be reflected within the processes for organizations described above, but in addition there are implications in terms of the way that the accountability governance chains will operate, the scope of risk assessment and the ways in which other stakeholders are able to hold this organisation to account. In complex, dynamic or global situations there needs to be a practical solution for data subjects to obtain both the requisite information about the service provision and remediation.

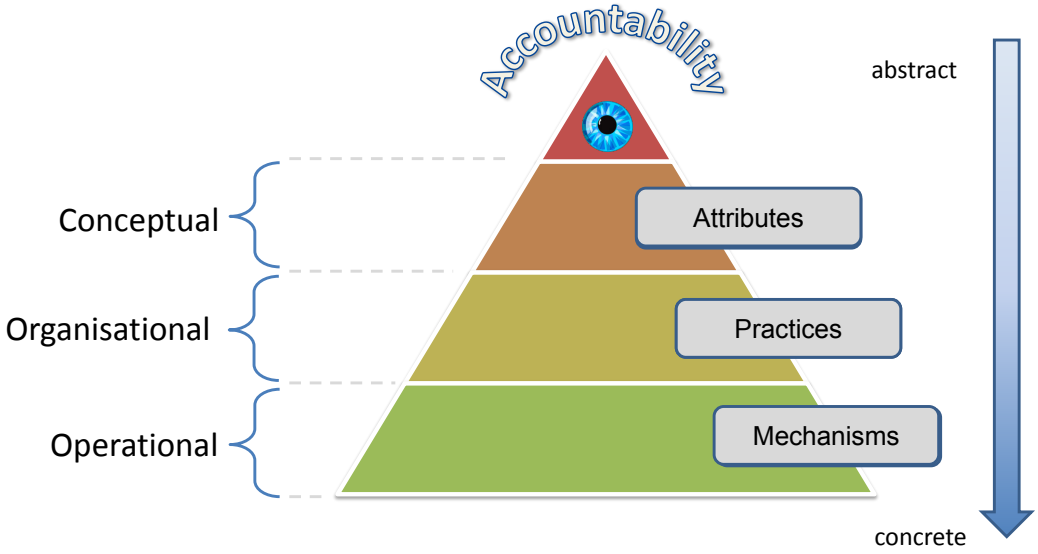

Figure 2: A Conceptual Framework for Accountability

6. Conceptual model

Our conceptual accountability model (see Figure 2) elaborates on the

definition provided in section 2 by means of a set of

- *Accountability attributes:* conceptual elements of accountability applicable across different domains (i.e., the conceptual basis for our definition, and related taxonomic analysis)

- *Accountability practices:* emergent behaviour characterising accountable organisations (that is, how organisations operationalise accountability or put accountability into practice)

- *Accountability mechanisms:* diverse processes, non-technical mechanisms and tools that support accountability practices (that is, accountability practices use them).

The model thus further operationalises the way accountability should be embedded in the cloud ecosystem's norms, practices and supporting mechanisms and tools. Importantly, the conceptual accountability model allows for changing patterns of accountable behaviour both in a top-down manner (e.g., enforcement of the legal framework), but also bottom-up (by providing various mechanisms that support accountability) within an entire cloud ecosystem. Moreover, it focuses upon both descriptive and normative accountability. On the one hand it sees to the specific social relation or the mechanism that involves an obligation to explain and justify conduct. Accountability attributes, practices and mechanisms are based on the "relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgment, and the actor can be sanctioned" (Bovens, 2007). On the other hand, the accountability attributes, practices and mechanisms not only aim to describe what to do (impose actions upon someone or an organisation), but also aim to stimulate actors' inherent feeling of being morally obliged to be responsive, open, transparent and responsible (Bovens, 2007). Behaving in an accountable or responsible manner then is perceived as a desirable quality and laid down in norms for the behaviour and conduct of actors. Based upon both the descriptive and normative approach to accountability, the objects of accountability can be established. Responsible data stewards are accountable for the following objects: norms (the obligations, permissions, prohibitions etc, that define (permissible) data practices), behaviour (the actual data processing behaviour of an organisation) and compliance (entails the comparison of an organisation's actual behaviour with the norms).

The core attributes of our accountability model are: transparency, responsiveness, remediability, responsibility, verifiability, appropriateness and effectiveness.

Transparency: the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.

Responsiveness: the property of a system, organisation or individual to take into account input from external stakeholders and respond to queries of these stakeholders.

Remediability: the property of a system, organisation or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms

Responsibility: the property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms

By "system" here we mean (parts of) the accountable cloud ecosystem, which could for example be a chain of cloud service providers or an IT process, which should be accountable to humans[8].

Being transparent is not only required with respect to the identified objects of the cloud ecosystem, the norms, behaviour and compliance, but also with respect to remediation[9]. Hence transparency can be argued to be the most important attribute of accountability. The remediation attribute assures that being transparent is not sufficient, and further action is required in order to be accountable[10]. Responsiveness is a key element of the notion of accountability in the relation between government and electorate (Mulgan, 2000) because ultimately, it is the electorate that mandates what happens (as in a social contract). In the context of cloud computing the providers are

[8]In a legal sense the entities further down the chain are not accountable to cloud customers, but rather to the entity one step up the chain, often the accountability property will relate to a single cloud service provider.

[9]This is not explicitly incorporated in the definition of transparency, because remediation can be seen as 'behaviour'.

[10]Without remediation, accountability would conflate with transparency.

private entities that determine their own actions, within the boundaries set by regulation, and if users do not like this, they can vote with their feet and refuse the service. However, even in the relation between cloud providers and their users, responsiveness is required. It refers to the two-way communication relation between cloud providers and external stakeholders (cloud users, regulator) needed within the cloud ecosystem to define part of the governing norms. In other words, the audience for an organisation's account must somehow be involved in the process by which the account is produced, and not only with the product (Raab, 2012). Responsibility differs from transparency, responsiveness and remediability, in that it assures that the state of being transparent, being responsive and willing and capable to remedy issues actually is assigned to the various stakeholders within the ecosystem.

Another key attribute that is a property of the objects of accountability (i.e., norm, behaviour, compliance) is:

Verifiability: the extent to which it is possible to assess norm compliance (i.e., a property of a system, service or process that its behaviour can be checked against norms)

Accountability is not a binary state, but rather a maturity state. This can be expressed by the attributes appropriateness and effectiveness, which act as indicators:

Appropriateness: the extent to which the technical and organisational measures used have the capability of contributing to accountability.

Effectiveness: the extent to which the technical and organisational measures used actually contribute to accountability.

By 'contribute to accountability', we mean (in the light of the analysis above) contribute to defining and displaying relevant norms, behaviour and compliance to the norms (i.e., comparing actual behaviour, intentions and results with the norms).

The accountability practices in the next layer of Figure 2 define the central behaviour of an organisation adopting an accountability-based approach, which we have already elucidated in Section 4 above and which in a general sense are defining governance, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly. Not only should an accountable organisation define and deploy policies regarding its data practices that meet regulatory, contractual

and normative obligations that apply to the context and are supported by senior management, but it should deploy mechanisms to put these policies in place, which are represented in the bottom layer of the diagram. Furthermore, accountable organisations must ensure that accountability extends through across their service supply chains, in other words ensuring that the services and partners they use are accountable too, which involves amongst other things proper allocation of responsibilities and provision of evidence about satisfaction of obligations along the service provision chain; this is not just a question of risk analysis involving both security risk assessment and also potential assessment of harm to individuals during provisioning and care when agreeing contracts, but also might involve taking into account the certification of partners against specific criteria to meet the accountability level needed for the context, with this mechanism including auditing and in some cases even continuous monitoring of this accountability level, probably involving third parties.

To support and implement the main accountability attributes, we have developed a 'toolkit' that forms the bottom layer in Figure 2 (accountability mechanisms), from which organizations can select as appropriate. The toolkit contains *extensions of existing business processes* like auditing, risk assessment and the provision of a trustworthy account, *non-technical mechanisms* like formation of appropriate organizational policies, remediation procedures in complex environments, contracts, certification procedures, and so on. We have defined a control framework which identifies key behaviours of accountable organisations (Gittler et al., 2015) [11]. Other components can be *technical tools*, which would include tracking and transparency tools, detection of violation of policy obligations, notification of policy violation, increased transparency without compromising privacy, and so on. The tools are targeted at different stakeholders, and some are designed for use as a preventive measure (for example, a Data Protection Impact Assessment to assess and reduce privacy harm before personal data is collected), some as a detective measure (for example, to assess policy violations) and others as a corrective measure (for example, to facilitate redress).

[11] The controls have been identified based on work done for the data protection domain (CNIL, 2012; ICO, 2012; Nymity Inc., 2014), augmented by more general organizational standards such as COBIT (ISACA, 2012) and ISO/IEC 27001 (ISO, 2013).

7. A Sketch of an Accountability Toolkit

The envisioned tools can be divided in four broad categories, corresponding with the objectives in Section 4: facilitating choice; enhancing control and transparency; monitoring and checking compliance; providing recommendations and guidance. We briefly elaborate on each of these by means of tools that are being developed within the A4Cloud project.

7.1. Objective 1 – Facilitating Choice

Cloud end users should be enabled to make informed choices about cloud services and how these may use and will protect their data in the cloud. A first requirement for an organisation entering the cloud is to establish the privacy and data protection risks involved in their operation, and for this we have developed the Data Protection Impact Assessment tool (DPIAT). This tool (Alnemr et al., 2015), comprising some 60 questions, helps the organisation to get a clear picture of their risks and provides a stepping stone to achieve (European) data protection regulation compliance[12]. An additional tool (i.e., the Cloud Offerings Advisory Tool (COAT) (Alnemr et al., 2014)) allows customers of cloud services to express their privacy and security preferences based on the type of data that will be involved prior to engaging with an actual service provider. The tool then matches known cloud service offerings with these preferences to facilitate customers to make informed choices regarding cloud providers. This tool supplements existing cloud brokerage tools that focus on price and performance by focusing on the degree of accountability – in view of privacy, security, and data protection – offered.

The main differentiation between the existing body of research and our Cloud Offerings Advisory Tool (COAT) is the focus of the latter on elucidation, explanation and comparison of privacy and security-related non-functional requirements that are reflected in different cloud service offerings. In particular, we broaden out the domain of assessment to include the potential harm to data subjects (DPIAT) and differences in contractual promises

[12]The DPIAT is developed in view of the upcoming General Data Protection Regulation and takes a two step approach: first a risk assessment to determine whether the full blown DPIAT is required. If so, then step two comprising the complete impact assessment is performed.

from a data protection perspective (e.g., jurisdiction of court, data retention period, notification channel and triggers, etc.) (COAT).

Ouedraogo and Mouratidis (2013) advocate the C.A.RE approach which enables assessment of security assurance provided by cloud service providers and guides cloud customers in selecting appropriate providers, involving assessment of the portion of the key security requirements of a standard, regulatory or relevant policies that are covered by the cloud service provider to security. Part of the justification that appropriate measures have been used comes from an enhanced risk assessment process. The role of a risk-based approach in data protection has been considered by a number of parties, including: as an assessment of the relative values of such an approach (Bennett and Raab, 2006); modifying the data protection principles to take this into account (OECD, 2013) and recent regulatory analysis (CIPL, 2014; DG Justice, 2014).

7.2. Objective 2 – Control and Transparency

An accountable cloud service provider must provide its users with (most likely, more) control over the service arrangement and data handling. This includes more opportunities for (dynamic) negotiation of (security) service level agreements (SLAs), including such aspects of who may do what with the customer's data. The A4Cloud project has further developed the PrimeLife Policy Language (PPL) developed in the EU FP7 project PrimeLife to express these data handling policies in cloud environments (Accountability PPL (A-PPL) (Azraoui et al., 2015)). The policies expressed in A-PPL can be enforced by the A-PPL-Engine.

Furthermore, cloud providers must demonstrate and provide evidence that the (negotiated) obligations are also met downstream throughout the service provision chain. Finally it must be ensured that the demonstration of compliance and other communications are made unambiguous and understandable by the target stakeholders (especially for small and medium enterprises (SMEs) and individuals). Data Track (Fischer-Hübner et al., 2014), which is designed to be an end-user tool, facilitates this kind of transparency.

The value of security transparency and mutual audit is confirmed by Ouedraogo et al. (2015), who advocates both ranking providers according to their level of transparency (see Objective 1 above), and ensuring that cloud services are designed and engineered with transparency in mind. To the first end, Pauley (2010) presented a checklist that cloud customers can use to evaluate the degree of transparency a given provider offers, although our

research has shown that not all of the categories are considered relevant in a European context (Cruzes and Jaatun, 2015).

Cloud providers must provide a proof of appropriateness of the procedures and mechanisms that are used to provision the service, e.g., to prove that the procedures and mechanisms are appropriate to the context. A certification system would be one way of approaching this (Prüfer, 2013).

7.3. Objective 3 – Compliance

Compliance of behaviour with the norms and policies governing the data handling can partly be enforced by technical tools, such as the A-PPL-Engine. However, we have seen that preventive mechanisms are not enough on their own. The Audit Agent System (AAS) collects evidence through software agents and provides an automated audit service based on compliance with custom-defined policies (Doelitzscher et al., 2013). For this purpose it automatically and continuously collects and analyses evidence produced by software agents in the system against the defined policies. For example, an AAS plug-in is being developed to monitor changes to key configuration files. The AAS resembles tools developed within comparable other audit initiatives like CSA's STAR initiative, ENISA's Assurance Framework or ISACA's Cloud Computing Management Audit/Assurance Program (Halpert, 2011). However, demonstrating compliance in A4Cloud is no longer part of self-assessment (by CSPs) (e.g., CSA's STAR[13] self-assessment), or initiated by relevant stakeholders (customers, data subjects, regulators), but an inherent characteristic of the A4Cloud system due to its implementation in the ecosystem.

AAS is complemented by the Data Transfer Monitoring Tool (DTMT) which collects evidence about how data transfers comply with obligations specified in policies (De Oliveira et al., 2013). These tools contribute to a proactive approach to compliance monitoring, and could eventually be included in new continuous compliance frameworks, such as CSA STAR Continuous. Another aspect is to provide proof of how the cloud providers' policies satisfy external criteria such as relations to law enforcement agencies; this also includes social norms regarding what kind of data may be stored and processed, and how this data may be accessed by the provider.

[13]https://cloudsecurityalliance.org/star/

Importantly, non-compliance and incidents[14] not only have to be detected, but have to be reported to relevant stakeholders (customers, data subjects, regulators) and those affected should be able to take action to mitigate harms and/or initiate redress. An Incident Management Tool (IMT) (Jaatun and Tøndel, 2015) receives notifications of security incidents and policy violations[15] through the other tools (e.g., AAS, the policy engine, etc.), parses the information received, and when end-user customers are involved sends it to the Redress & Remediation Tool (RRT). RRT, a plugin living in Data Track, has the following functions:

- informs users what happened in a comprehensible, human-readable format
- provides a signed and time-stamped .pdf containing a trustworthy report, which we envision the user can bring to a lawyer to serve in legal proceedings
- provides a log containing technical, non human-readable details on the incident, which would ideally function as evidence
- provides a list of actions that the user can undertake to remedy the incident, such as 'change password' or inform bank to block credit card

The information may be made available to relevant regulators, such as the Data Protection Authorities through for instance dedicated messages.

Security Information and Event Management (SIEM or SIM/SEM) solutions have a critical role in monitoring operational security and supporting organisations in decision-making. They provide a standardised approach to collect information and events, store and query and provide degrees of correlations, usually driven by rules (Kavanagh et al., 2014). SIEM solutions do not cover business audit and strategic (security) risk assessment but instead provide inputs that need to be properly analysed and translated into a suitable format to be used by senior risk assessors and strategic policy makers. Risk assessment standards such as ISO 2700x (ISO, 2013), NIST SP800-30 (NIST, 2012), etc. operate at a macro level and usually do not fully utilise

[14]Such as data breaches, unauthorised access, unduly moved virtual machines, misconfiguration of technical protection measures, and unavailability of the service.

[15]Including violations of both user-set and regulatory policies.

information coming from logging and auditing activities carried out by Information Technology (IT) operations. Similarly, there exist a number of frameworks for auditing a company's IT controls, most notably COSO[16] and COBIT (ISACA, 2012).

Other types of detective mechanisms are concerned with cloud service usage rather than security and information monitoring. There exists a class of evidence-related cloud technologies that provide generic mechanisms supporting basic logging and monitoring – for example, Sumologic[17], Amazon Web Services (AWS) CloudTrail[18] and Logentries[19].

Different security controls can be identified that organisations need to implement in the cloud (see for example NIST SP500-299 (NIST, 2013)). From a management viewpoint, it is possible to identify critical processes (e.g., security risk assessment and privacy management) that address the mitigation of security and privacy threats (Nymity Inc., 2014) and the essential elements of a good organisational privacy management programme have been defined (OPC, 2012). Certification can be an important aspect of such frameworks. ENISA has developed a Cloud Certification Schemes Metaframework (CCSM) that classifies different types of security certification (that are aligned with specific standards) for cloud providers (Dekker and Liveri, 2014). This meta-framework is used to compare a number of different certifications identified within the Cloud Certification Schemes List (CCSL). The overall objective of this framework is to make the cloud more transparent for cloud customers, in particular, in the way cloud providers meet specific security objectives.

7.4. Objective 4 – Recommendations and guidelines

Accountability goes beyond technical tools. Cloud customers (especially SMEs), end-users, and also cloud service providers need to be educated on what responsible stewardship of data means and how this can be accomplished. Recommendations and guidelines help raise this awareness and also support organizing and handling affairs. To this purpose the project has pro-

[16] http://www.coso.org
[17] http://www.sumologic.com
[18] http://aws.amazon.com/cloudtrail/
[19] https://logentries.com/

vided deliverables[20] outlining the conceptual framework (Felici et al., 2014), requirements for accountability (Cruzes et al., 2014), legal reports (Hon et al., 2014), including reports with best practices for cloud contracts.

Since cloud computing does not only affect customers and end-users, but also society at large, a more democratic approach to accountability, involving the public at large, is desirable. Increasingly it is argued that access to the Internet should be perceived as a human right (e.g., as discussed by Wicker and Santoso (2013) or La Rue (2011)). Especially since cloud computing embodies the digitalization of society and enforces organizational (new ways of living our lives, perform work, do business and administer public tasks and services) and societal changes (towards a "better" society) (de Pous, 2012). Democratic accountability refers to the many ways in which citizens, political parties, parliaments and other democratic actors can provide feedback to and reward or sanction cloud providers. Well-functioning accountability mechanisms are believed to provide incentives for cloud providers to work in the best interests, not only of their customers and own employees, but also of citizens.

Ensuring democratic accountability entails that transparency should also be aimed at the general public and the regulator. This could take the shape of transparency reports published by cloud providers, as is currently already the case with respect to law enforcement requests by some large Social media (e.g., Facebook) and content hosting companies (such as Microsoft and Apple) and 'Right to be Forgotten' requests by Google. Moreover, responsiveness is extended to include the general public, whether or not represented by consumer organisations or parliamentary members. A4Cloud project deliverables and publications like this paper convey the message to Cloud providers that they should take into account the views and concerns of these stakeholders as well. As such, transparency and responsiveness may contribute to the sustainability of the cloud ecosystems in the long run. In addition, democratic accountability provides a reflective attitude contributing to the continuous monitoring process. This, in its turn, contributes to the maintenance of ethical standards, rather than stimulating a race to the bottom (of cost and privacy protection).

[20]All public A4Cloud deliverables can be downloaded from `http://www.a4cloud.eu/deliverables`.

8. Discussion

That Cloud computing has transformed the way many organizations work and offers added value for operation management and service computing is widely acknowledged. Nevertheless, the inherent ubiquitous nature of the Cloud has also introduced a more complicated, networked and global environment for international data transmissions. This cloud environment is so complex that despite the reported benefits, there are still many (perceived) risks that refrain potential customers from using cloud services (Catteddu and Hogben, 2009). The accountability model, as proposed by the A4Cloud project, provides an elaborated approach to solving / diminishing these risks based upon the stimulation of responsible stewardship and mechanisms that allow cloud users to control what happens with their data. We furthermore explore the inclusion of "accountability" in the market system of cloud computing as a valuable and commercial asset for cloud providers (Prüfer, 2013).

We explicitly place our notion of accountability in the context of privacy and security. Privacy should not be read in the classical Warren and Brandeis (1890) interpretation of "the right to be let alone". Maybe we have not so much lost the right to be let alone, but we have lost the capacity to go unmonitored, given that we base so much of our existence on interaction and communication with others over the internet (Jaatun et al., 2012). The buck does not stop here. Big data analytics on browsing and purchase history and other metadata allow ad brokers, internet retailers and other major players to infer much more about their users than what they are volunteering (Podesta et al., 2014). In some cases, this allows a service provider to identify individual users even when they are using the service anonymously (Ohm, 2010).

Nowadays, given the flight that social media and the cloud have taken, seclusion no longer seems the most prominent privacy dimension. Instead, Westin's notion of informational privacy 'a right to control one's personal data; who gets to see what of us' (Westin, 1967), has gained importance. This interpretation has found its way in, for instance, the European Data Protection Directive (European Parliament, 1995). Accountability is embedded in this legal framework, through concepts such as purpose specification and transparency provisions. Accountability does not equal privacy, but can contribute to informational privacy and is actually mandated by law.

The big Cloud providers that currently dominate the international market have such economic power that they can effectively ignore any European

attempts at forcing them to run their business the way the European Union (EU) thinks they should. It seems European privacy regulators "speak loudly, but carry a small stick"[21] as exemplified by CNIL's recent fining of Google – 150 000 euros is hardly something Google will lose sleep over (CNIL, 2014).

The upcoming General Data Protection Regulation (European Commission, 2012) will further consolidate accountability (and compliance) into the legal framework. This will not only provide a strong regulatory push towards stronger accountability in the EU (the proposed fines for non-compliance are very stiff[22] [23], but likely due to what is called 'the Brussels effect' (Bradford, 2012), proliferate beyond the EU. The framework and tools discussed in this paper enable Cloud providers to comply.

Our message, however, goes beyond this functional approach. Accountability can increase customer trust in online services. Adopting an accountability approach means as we have outlined accepting responsible stewardship for data. This is a moral stance. Accountability then is demonstrating to relevant stakeholders that one "does the right thing" and that one accepts the consequences if things go wrong. This may provide a strong selling point. The Snowden revelations have caused ripples in people's and organisations' trust in information services (see for instance (Preibusch, 2015)). The opaqueness of what happens in the cloud and who has access to what data is part of this distrust. Accountability and its constituent elements may help restore trust in this domain. The tools and mechanisms presented in this paper contribute to making strong accountability possible.

What we have presented is only part of the puzzle for modern services. The kind of tools that we have outlined in Section 7 will need to be complemented by other security tools to make security and privacy stronger, for instance by enforcing confidentiality and anonymity where desired. Accountability is 'merely' a cross-cutting concern alongside privacy and security within cloud and future internet services

[21] In contrast to Theodore Roosevelt's popular quote "Speak softly, and carry a big stick, you will go far" http://www.loc.gov/exhibits/treasures/images/at0052as.jpg.

[22] The discussions in the Trilogue converged around 2-5 % of global annual turnover. That does make it boardroom material.

[23] Strong accountability describes 'an approach that applies not only to policies and procedures, but also to practices, so that the effectiveness of the processing of personal data can be overseen (this stresses a distinction between 'reporting' and 'demonstrating') (Butin et al., 2014).

While we believe that the importance of confidentiality and privacy enhancing technologies (Jaatun et al., 2012) will continue to increase in the years to come, we also agree with Weitzner et al. (2008) that the "hide it or lose it" perspective on information security is insufficient for many use cases in the Cloud. Digital information is so easily copied, and security mechanisms have so many caveats that it is often not possible to guarantee privacy by technical means alone. Schneider (2009) supplements this by pointing out the complexity of computer systems, something which is often compounded by the lack of clear specifications, articulated environmental assumptions, and informed threat analysis. He rightly asserts that ensuring responsibility in case of misbehaviour is easier than preventing it in the first place. This boils down to that we as users need to trust the provider, but the providers must give us *reason* to trust them. To quote Weitzner et al.:

> Information Accountability means that information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules (Weitzner et al., 2008).

We are extending Weitzner et al.'s approach by also providing preventive measures, but since the vast information resources available to a Cloud provider potentially enables them to infer sensitive information about their users (as noted above), we believe it is equally important for the providers to be upfront about the kind of information that is available to them, what they use it for, and how it is shared with others.

9. Conclusion

We believe that much can be achieved by the providers taking a more conscious approach to data stewardship. In this paper we have presented fundamental requirements that we believe must be met by Cloud providers wishing to be accountable stewards of their customers' data.

The kinds of tools we have outlined in Section 7 all contribute to an accountability-based approach, increasing transparency for Cloud users, and enabling Cloud providers to "do the right thing" with respect to accountability along the provider chain. While we have no illusions about in any way being in a position to force Cloud providers to use our (or indeed any) accountability solution, we believe that providers soon will be required to justify their practices and mechanisms for handling customers' data to external parties (Pearson, 2013), and that a certification scheme inevitably will

emerge, much like we see for the Payment Card Industry Data Security Standard (PCI-DSS) (PCI Security Standards Council, 2013). This implies that new standards in this space will be necessary, building on existing efforts by, e.g., the European Union Agency for Network and Information Security (ENISA), Cloud Security Alliance (CSA), and the International Standards Organization (ISO).

Acknowledgements

This work has been partly funded from the European Commissions Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD) Cloud Accountability Project. We are grateful for the support of the A4Cloud project partners, in particular to the tool owners who are developing the accountability tools, and other people contributing to joint discussions on accountability attributes, notably Massimo Felici and Alain Pannetrat.

References

American Institute of Certified Public Accountants, 2016. SSAE 16 Overview.
URL `http://ssae16.com/SSAE16_overview.html`

Alnemr, R., Cayirci, E., Corte, L. D., Garaga, A., Leenes, R., Mhungu, R., Pearson, S., Chris Reed, A. S., Stefanatou, D., Tetrimida, K., Vranaki, A., 2015. A data protection impact assessment methodology for cloud. In: Annual Privacy Forum 2015.

Alnemr, R., Pearson, S., Leenes, R., Mhungu, R., Dec 2014. COAT: Cloud Offerings Advisory Tool. In: Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. pp. 95–100.

Ardagna, C. A., Camenisch, J., Kohlweiss, M., Leenes, R., Neven, G., Priem, B., Samarati, P., Sommer, D., Verdicchio, M., 2010. Exploiting cryptography for privacy-enhanced access control: A result of the prime project. Journal of Computer Security 18 (1), 123–160.

Azraoui, M., Elkhiyaoui, K., nen, M., Bernsmed, K., De Oliveira, A., Sendor, J., 2015. A-ppl: An accountability policy language. In: Garcia-Alfaro,

J., Herrera-Joancomart, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F., Suri, N. (Eds.), Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Vol. 8872 of Lecture Notes in Computer Science. Springer International Publishing, pp. 319–326.
URL http://dx.doi.org/10.1007/978-3-319-17016-9_21

Bennett, C., Raab, C., 2006. The Governance of Privacy: Policy Instruments in Global Perspective. MIT Press, Cambridge, Massachusetts.

Bennett, C. J., 2012. The accountability approach to privacy and data protection: Assumptions and caveats. In: Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo, H. (Eds.), Managing Privacy through Accountability. Palgrave Macmillan, Ch. 2, pp. 33–48.

Bier, E., Chow, R., Golle, P., King, T., Staddon, J., Nov 2009. The rules of redaction: Identify, protect, review (and repeat). IEEE Security & Privacy 7 (6), 46–53.

Bovens, M., 2007. Analysing and assessing accountability: A conceptual framework. European Law Journal 39 (4), 447–468.

Bradford, A., 2012. The Brussels effect. Northwestern University Law Review 107 (1), 1–68.

Butin, D., Chicote, M., Le Métayer, D., 2014. Strong accountability: Beyond vague promises. In: Serge Gutwirth, Ronald Leenes and Paul De Hert (Ed.), Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Springer.

Cattaneo, G., Kolding, M., Bradshaw, D., Folco, G., February 2012. Quantitative estimates of the demand for cloud computing in europe and the likely barriers to take-up. Tech. Rep. SMART 2011/0045 D2 Interim Report, IDC.

Catteddu, D., Hogben, G., 2009. Cloud Computing – Benefits, risks and recommendations for information security. ENISA Report.
URL https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Charlesworth, A., Pearson, S., 2013. Developing accountability-based solutions for data privacy in the cloud. European Journal of Social Science Research, Taylor and Francis, UK 26 (1), 7–35.

CIPL, October 2009. Data Protection Accountability: The Essential Elements - A Document for Discussion (the Galway project). Tech. rep., Centre for Information Policy Leadership, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

CIPL, October 2010. Demonstrating and measuring accountability - a discussion document - accountability phase ii (the paris project). Tech. rep., Centre for Information Policy Leadership.

CIPL, October 2014. A risk-based approach to privacy: Improving effectiveness in practice. Tech. rep., Centre for Information Policy Leadership.
URL http://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf

CNIL, 2012. Recommendations for companies planning to use cloud services.
URL http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

CNIL, 2014. The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc.
URL http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/

Cruzes, D., Jaatun, M. G., 2015. Cloud provider transparency - a view from cloud customers. In: Proceedings of the 5th International Conference on Cloud Computing and Services Science. pp. 30–39.

Cruzes, D. S., Jaatun, M. G., Felici, M., Haugset, B., Bernsmed, K., Gago, C. F., Reed, C., Leenes, R., November 2014. Requirements report. Tech. Rep. D:B-2.4, A4Cloud Project.

De Oliveira, A., Sendor, J., Garaga, A., Jenatton, K., Dec 2013. Monitoring personal data transfers in the cloud. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. Vol. 1. pp. 347–354.

de Pous, V. A., 2012. Cloud computing and public sector policy. Tech. rep., Victor de Pous.

Dekker, M., Liveri, D., November 2014. Cloud certification schemes metaframework.
URL https://resilience.enisa.europa.eu/cloud-computing-certification/Cloud_Certification_Schemes_Metaframework_version_1.2.pdf

DG Justice, 2014. Statement on the role of a risk-based approach in data protection legal frameworks. European DG of Justice (Article 29 Working Party), wP218.
URL http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Doelitzscher, F., Ruebsamen, T., Karbe, T., Reich, C., Clarke, N., 2013. Sun behind clouds - on automatic cloud security audits and a cloud audit policy language. International Journal On Advances in Networks and Services 6 (1&2).

Dybå, T., Dingsøyr, T., Moe, N. B., 2004. Process Improvement in Practice: A Handbook for IT Companies. International Series in Software Engineering (ISSN 1384-6469 ; 9). Springer.

EMS Corporation, 2016. Rsa archer governance, risk, and compliance.
URL http://www.emc2.la/security/rsa-archer-governance-risk-compliance/index.htm

European Commission, 2012. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
URL http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Parliament, 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.

URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Felici, M., Pearson, S., Dziminski, B., Gittler, F., Koulouris, T., Leenes, R., Niezen, M., Nuñez, D., Pannetrat, A., Royer, J.-C., Stefanatou, D., Tountopoulos, V., September 2014. Conceptual framework. Tech. Rep. D:C-2.1, A4Cloud Project.

Fischer-Hübner, S., Angulo, J., Pulls, T., 2014. How can cloud users be supported in deciding on, tracking and controlling how their data are used? In: Hansen, M., Hoepman, J.-H., Leenes, R., Whitehouse, D. (Eds.), Privacy and Identity Management for Emerging Services and Technologies. Vol. 421 of IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, pp. 77–92.
URL http://dx.doi.org/10.1007/978-3-642-55137-6_6

Gittler, F., Haddad, M., Koulouris, T., Pearson, S., Tountopoulos, V., Önen, M., Azraoui, M., Bernsmed, K., Brown, M., Elkhiyaoui, K., Gago, C., Gleeson, N., Luna, J., Núñez, D., Pannetrat, A., Royer, J., Santana De Oliveira, A., Sellami, M., Vranaki, A., October 2015. Cloud accountability reference architecture. Tech. rep., a4Cloud Project deliverable.
URL http://www.a4cloud.eu/content/cloud-accountability-reference-architecture

Halpert, B., 2011. Auditing Cloud Computing: A Security and Privacy Guide. Vol. 21. John Wiley & Sons.

Hon, K., Kosta, E., Millard, C., Stefanatou, D., February 2014. White paper on the proposed data protection regulation. Tech. Rep. D:B-5.1, A4Cloud Project.

Hood, C., 2010. Accountability and transparency: Siamese twins, matching parts, awkward couple? West European Politics 33 (5), 989–1009.

ICO, 2012. Guidance on the use of cloud computing. Information Commissioner's Office.

Informatica, 2013. Informatica dynamic data masking. Data Sheet.
URL https://www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/data-sheet/dynamic-data-masking_data-sheet_1779.pdf

ISACA, 2012. COBIT: Control Objectives for Information and related Technology.

ISO, 2013. Information technology – security techniques – information security management systems – requirements. ISO/IEC Std. 27001:2013.

Jaatun, M. G., Nyre, Å. A., Tøndel, I. A., Bernsmed, K., 2012. Privacy Enhancing Technologies for Information Control. In: Yee, G. M. (Ed.), Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards. IGI Global, pp. 1–31.

Jaatun, M. G., Pearson, S., Gittler, F., Leenes, R., Dec 2014. Towards strong accountability for cloud service providers. In: Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. pp. 1001–1006.

Jaatun, M. G., Tøndel, I. A., 2015. How much cloud can you handle? In: Availability, Reliability and Security (ARES), 2015 10th International Conference on. pp. 467–473.

Jones, S., 2015. Cloud computing procurement and implementation: Lessons learnt from a united kingdom case study. International Journal of Information Management 35 (6), 712 – 716.
URL http://www.sciencedirect.com/science/article/pii/S0268401215000699

Kavanagh, K. M., Nicolett, M., Rochford, O., 2014. Magic quadrant for security information and event management. Gartner report.

La Rue, F., 2011. Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. Tech. rep., United Nations General Assembly.
URL http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Lampson, B. W., 2004. Computer security in the real world. Computer 37 (6), 37–46.

Mell, P., Grance, T., Sep 2011. The NIST Definition of Cloud Computing. Special publication 800-145, NIST.

Miller, A., Horne, R., Potter, C., 2015. Information security breaches survey 2015. Commissioned by HM Government, conducted by PwC in association with Infosecurity Europe and Reed Exhibitions.
URL http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

Mulgan, R., 2000. "accountability": An ever-expanding concept? Public Adm 78, 555–573.

NIST, September 2012. Guide for conducting risk assessments. NIST Special Publication 800-30 Revision 1, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

NIST, 2013. NIST Cloud Computing Security Reference Architecture. NIST Special Publication 800-299 (Draft).

Nymity Inc., 2014. Privacy management accountability framework.

OECD, 2013. Organisation for Economic Co-operation and Development.
URL http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Ohm, P., 2010. Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review 57, 1701–1777.

OPC, April 2012. Getting accountability right with a privacy management program. 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.
URL https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf

Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S., Dubois, E., 2015. Security transparency: the next frontier for security research in the cloud. Journal of Cloud Computing 4 (1), 1–14.
URL http://dx.doi.org/10.1186/s13677-015-0037-5

Ouedraogo, M., Mouratidis, H., 2013. Selecting a cloud service provider in the age of cybercrime. Computers & Security 38, 3 – 13, cybercrime in the Digital Economy.

URL http://www.sciencedirect.com/science/article/pii/S0167404813000242

Pauley, W., Nov 2010. Cloud provider transparency: An empirical evaluation. Security Privacy, IEEE 8 (6), 32–39.

PCI Security Standards Council, 2013. Payment Card Industry Data Security Standard.
URL https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0

Pearson, S., 2013. On the relationship between the different methods to address privacy issues in the cloud. In: Meersman, R., Panetto, H., Dillon, T., Eder, J., Bellahsene, Z., Ritter, N., Leenheer, P., Dou, D. (Eds.), On the Move to Meaningful Internet Systems: OTM 2013 Conferences. Vol. 8185 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 414–433.
URL http://dx.doi.org/10.1007/978-3-642-41030-7_30

Pearson, S., Tountopoulos, V., Catteddu, D., Sudholt, M., Molva, R., Reich, C., Fischer-Hubner, S., Millard, C., Lotz, V., Jaatun, M., Leenes, R., Rong, C., Lopez, J., 2012. Accountability for cloud and other future internet services. In: Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. pp. 629–632.

Podesta, J., Pritzker, P., Moniz, E. J., Holdren, J., Zients, J., May 2014. Big data: Seizing opportunities, preserving values. Tech. rep., Executive Office of the President.

Preibusch, S., 2015. Privacy behaviors after Snowden. Communications of the ACM 58 (5), 48–55.

Prüfer, J., Dec 2013. How to Govern the Cloud? Characterizing the Optimal Enforcement Institution that Supports Accountability in Cloud Computing. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. Vol. 2. pp. 33–38.

Raab, C., 2012. The meaning of the word "accountability" in the information privacy context. In: Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo, H. (Eds.), Managing Privacy through Accountability. Palgrave Macmillan.

Rong, C., Nguyen, S. T., Jaatun, M. G., 2013. Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering 39 (1).
URL http://www.sciencedirect.com/science/article/pii/S0045790612000870

Schneider, F. B., 2009. Accountability for perfection. IEEE Security & Privacy 7 (2), 3–4.

Steijn, W. M. P., Niezen, M. G. H., Dec 2015. The Value of Accountability in the Cloud – Individual Willingness to Pay for Transparency. IEEE Technology & Society Magazine 34 (4), 74–82.

Warren, S. D., Brandeis, L. D., 1890. The Right to Privacy. Harvard Law Review, 193–220.

Webster, N., 1828. American Dictionary of the English Language. Merriam-Webster.
URL http://webstersdictionary1828.com/

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G. J., 2008. Information accountability. Communications of the ACM 51 (6).
URL http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf

Westin, A. F., 1967. Privacy and Freedom. International Series in Software Engineering (ISSN 1384-6469 ; 9). Atheneum.

Wicker, S. B., Santoso, S. M., 2013. Access to the internet is a human right. Communicaitons of the ACM 56.

Wiener, N., 1948. Cybernetics: Or Control and Communication in the Animal and the Machine. MIT Press.