Towards Accountability in the Cloud

Siani Pearson

HP Laboratories
HPL-2011-138

Keyword(s):

accountability; cloud; obligation; trust; privacy; responsibility; transparency

Abstract:

Accountability is likely to become a core concept in the cloud and to underpin new mechanisms that help increase trust in the cloud. These mechanisms must be applied in an intelligent way, taking context into account and avoiding a 'one size fits all' approach.

External Posting Date: September 6, 2011 [Fulltext] Approved for External Publication
Internal Posting Date: September 6, 2011 [Fulltext]
Published as Siani Pearson, "Toward Accountability in the Cloud", View from the Cloud, IEEE Internet Computing, IEEE Computer Society, July/August issue, vol. 15, no. 4, pp. 64-69, 2011.

Towards Accountability in the Cloud

Siani Pearson - HP Labs

Abstract

Accountability is likely to become a core concept in the cloud and to underpin new mechanisms that help increase trust in the cloud. These mechanisms must be applied in an intelligent way, taking context into account and avoiding a 'one size fits all' approach.

Article

A commonly-accepted definition for cloud computing is provided by US National Institute of Standards and Technologies: "Cloud computing is a model for enabling 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." Cloud provides a market opportunity with a huge potential both for efficiency and new business opportunities (especially in service composition), and is almost certain to deeply transform our IT. Not only are there cost savings due to economies of scale on the service provider side and pay-as-you-go models, but business risk is decreased because there is less need to borrow money for upfront investment in infrastructure.

However, to help realise these benefits, we need to address two potential barriers: lack of consumer trust and the complexity of compliance.

Lack of consumer trust is commonly recognised as a key inhibitor to moving to Software as a Service (SaaS) cloud models. People have increasing expectations that their data will be handled in a responsible way and will be protected by the companies they choose to share data with. Furthermore, compared to traditional server architectures, cloud consumers are more concerned about the integrity, security and privacy of their data, as there is a shift from a server-health perspective to a data perspective. However, current terms of service push back risk to consumers and offer very little remediation or assurance. Furthermore, there is a perceived lack of transparency and relatively less control compared to traditional models, and this is of particular concern for sensitive information. There have also been some cases where Cloud Service Providers (CSPs) have been forced by subpoenas to hand over data stored in the cloud, and there is a fear that governments might also be able to get access to information stored in servers within their countries. Moreover, it is not clear what would happen if things go wrong. Would a cloud user be notified if a privacy breach had occurred, and who would be at fault in such cases? It can be much more complex to work out how redress could be obtained, and also hard to ascertain if data has been properly destroyed in case of change or bankruptcy of cloud provider. So people are concerned about weak trust relationships along the chain of service provision, especially 'on demand' models where CSPs may have to be found quickly, and as a result it is not true that trust will be transitive right along the chain.

The second barrier to migration to cloud models is the difficulty of compliance for CSPs. A major reason for this is that data flows tend to be global and dynamic. As location matters from a legal point of view, this leads to regulatory complexity. It can be difficult to comply with legislation, especially transborder data flow requirements, and even to determine which laws apply and which courts should preside. Issues such as unauthorised secondary usage of data and inappropriate retention of data also can be difficult to address.

These two issues – trust and complexity - are closely linked: CSPs have both legal and ethical obligations to ensure privacy and protect data, and thereby demonstrate the trustworthy nature of their services.

The advantages of cloud computing can result in a higher risk to privacy and security, as we have seen above when discussing the danger of non-compliance , where issues faced in subcontracting and offshoring can be magnified. It is not just consumers who are worried about privacy and security concerns in the cloud [1]. The European Network and Information Security Agency (ENISA)'s cloud computing risk assessment report [2] states 'loss of governance' as one of the top risks of cloud computing, especially for Infrastructure as a Service (IaaS). 'Data loss or leakages' is also one of the top seven threats listed by Cloud Security Alliance in their 'Top Threats to Cloud Computing Report' [3]. The autonomic and virtualized aspects of cloud can bring new threats, such as cross-VM side channel attacks, or vulnerabilities due to data proliferation, dynamic provisioning, the difficulty in identifying the location of physical servers or the lack of standardisation. Although service composition is easier in cloud computing, the source of services may be malicious. However, privacy and security risks may actually be decreased compared to traditional models if CSPs with expertise in privacy and security are used.

In this article I argue that the notion of accountability is key to addressing these issues. It is especially helpful for protecting sensitive or confidential information, enhancing consumer trust, clarifying the legal situation in cloud computing and facilitating cross border transfers of data. Our focus here is on data protection issues in the cloud. The meaning of 'data protection' has rather more of a privacy focus in Europe, but a broader data security context in US. We focus on privacy, but some of these issues do transcend personal data handling and generalize to other types of data, beyond privacy concerns.

It is likely that over time, legislation will put more emphasis on accountability: the move to cloud (and related changes) has been straining traditional legal frameworks. We discuss in the next section how right over the world, our current laws are likely to be revised, with accountability a central feature of these new laws.

What is accountability?

First we consider what accountability is. The term has been used for a number of years in computer science to refer to a narrow and imprecise requirement that is met by reporting and auditing mechanisms. In this article, the context of its use is corporate data governance. Accountability (for complying with measures that give effect to the practices articulated in the guidelines) has already been

present in core frameworks for privacy protection, most notably the Organisation for Economic Cooperation and Development (OECD)'s privacy guidelines (published in 1980), Canadian PIPEDA legislation (that received royal assent in 2000) and Asia Pacific Economic Cooperation (APEC)'s Privacy Framework (endorsed in 2005).

More recently, region block governance models are evolving further to incorporate accountability and the responsible use of information, and regulators are increasingly requiring that companies prove they are accountable. In particular, frameworks like the European Union (EU)'s Binding Corporate Rules (BCRs) and APEC Cross Border Privacy Rules are being developed to provide a cohesive and more practical approach to data protection across disparate regulatory systems, and this is a new development. For example, BCRs require that organisations demonstrate that they are, and will be, compliant with requirements defined by EU Data Protection Authorities (DPAs) for transferring data outside EU. More recently, the significance and utility of the principle of accountability in introducing innovations to the current legal framework in response to globalization and new technologies has been highlighted in "The Future of Privacy", released by the Article 29 Working Party in December 2009, The Opinion of the Article 29 Working Party released in July 2010, and the global data protection standards of the Madrid Resolution (adopted by the International Conference of Data Protection and Privacy Commissioners in October 2009).

The 'Galway project' of privacy regulators and privacy professionals provides a reasonable definition of accountability, in the context of this latest regulatory sense, when it says [4]: "Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."

Central components of this notion are transparency, responsibility, assurance, and remediation. In terms of responsibility, organizations need to demonstrate acknowledgement and assumption of responsibility, both in terms of having in place appropriate policies and procedures, and in terms of promoting good practices that include correction and remediation for failure and misconduct. Responsible decision making should be used, and in particular organizations should report, explain and be answerable for the consequences of decisions about the protection of data.

In order to provide accountability, it has been argued that a shift is needed from hiding information to ensuring that only appropriate uses occur [5]. Information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules. A history of data manipulations and inferences can be maintained (providing transparency) and can then be checked against a set of policies that are supposed to govern them (providing accountability). This provides retrospective accountability, in the sense that if actor A performs action B then we can review B against a predetermined policy to decide if A has done something wrong, and so hold A accountable.

We want to extend this approach to include prospective effects, for example, because the environment may change. We want to reduce the risk of disproportionate harm to data subjects, and thereby reduce negative consequences for the data controller(s). To do this, we build in processes and reinforce good

practices such that liability does not arise in the first place [6]. This is a reflexive privacy process, which is not static and where there is an ongoing assessment of harm and process of privacy review throughout the contractual/service provision chain.

Broadly speaking, an accountability approach in accordance with current regulatory thinking requires organizations to:

1. commit to accountability and establish policies consistent with recognized external criteria
2. provide transparency and mechanisms for individual participation, for example including sharing these policies with stakeholders and soliciting feedback
3. use mechanisms to implement these policies: including clear documentation and communication (encompassing the organisation's ethical code), gaining support from all levels within the organizational structure, tools, training, education, ongoing analysis and updating
4. allow validation: provide means for external enforcement, monitoring, and audit
5. provide mechanisms for remediation: these should include event management (e.g. dealing with data breaches) and complaint handling.

We argue that item 3. above can be extended to encompass both pre-emptive approaches (to assess risk and avoid privacy harm) and reactive approaches that provide transparency and audit. And the privacy policies and mechanisms need to take into account the entire life cycle. Companies need to think about what data they will collect and how they plan to use it, but also what are the potential harms (or surprises) for individuals. It is the data subject that is the real owner of data, who ultimately is harmed in case of failure and who should be empowered and supported. For example, if you are tracking someone online then under an accountability approach you might include clear notice that tracking is happening, how the tracking data will be used, a mechanism for individuals to choose not to be tracked and to request previous tracking data to be deleted.

Data stewardship

A closely related notion is data stewardship. In a cloud model , IT is consumed from many different cloud providers in an ecosystem. It is a challenge to understand such ecosystems, and a step change in thinking is required. Security and privacy management evolves into an information stewardship problem. In the cloud, it will be harder to establish the risks and obligations, implement appropriate operational responses and deal with regulatory requirements. The notions of transparency and assurance come in more strongly and it is necessary to ensure 'chains of accountability'. Accountability places a legal responsibility upon an organization that uses personal information to ensure that the contracted partners to whom it supplies the personal information are compliant, wherever in the world they may be. So, the communities responsible for data stewardship (who are typically organisational IT security, legal, operations and compliance staff) place responsibilities/constraints on other individuals or on the way systems operate, and these constraints are met along the chain of provision.

In our Lab we have explored the notion of data stewardship in a broader context than just personal information - in the UK-funded Cloud Stewardship Economics project we are currently modelling the

economics of information stewardship in cloud computing ecosystems, making explicit both the expectations and responsibilities of cloud stakeholders and the design assumptions of systems [7].

The need for intelligent accountability

The idea of 'intelligent accountability' was first proposed by Baroness O'Neill in her 2002 Reith Lectures on 'A Question of Trust', as a means to provide greater accountability without damaging professional performance. She argued that much that has to be accounted for is not easily measured and cannot be reduced to a set of stock performance indicators. She said that intelligent accountability "requires more attention to good governance and fewer fantasies about total control" and "Good governance is possible only if institutions are allowed some margin for self-governance of a form appropriate to their particular tasks".

We need to introduce accountability in an intelligent way, or else trust will not increase and the overall effect can be quite negative in terms of the increased administrative burden. As relates to the cloud, intelligent accountability could involve:

- Moving away from 'box checking' and static privacy mechanisms
- Assessing potential harms to data subjects before exposing data to risks. This would be part of ongoing risk assessment and mitigation, for which Privacy Impact Assessments (PIAs) are one important tool
- Allowing organizations more flexibility in how to provide data protection – so that they can use internal mechanisms and controls that make most sense for their business situation rather than a 'one size fits all' prescriptive set of rules
- Various degrees of accountability – it may be that more stringent standards and tests for accountability could facilitate proof of the CSPs' readiness to engage in certain activities (such as those that involve processing highly sensitive data) or even allow them to be relieved of certain administrative burdens (such as re-notification of minor changes in processing)
- Development of clever, automated analysis, automated internal policy enforcement and other technologies to enhance enforcement and avoid increasing the human burden (this is discussed further in the following section)

As an integral part of this approach, organizations will need to spend time and resource analyzing what this means to them and gaining the management support to implement necessary changes.

How to provide accountability in the cloud

Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data. Legislation and policies tend to apply at the data level, but the mechanisms can be at various levels, including the system level and data level. A toolbox of measures could be provided for data controllers, to allow construction of custom-built solutions, whereby the controllers might tailor measures to their context (taking into account consideration of the systems involved, type of data, data flows, etc).

We can co-design legal mechanisms, procedures and technical measures to support this approach. We may integrate design elements to support:

- prospective (and proactive) accountability, using preventive controls
- retrospective (and reactive) accountability, using detective controls

Preventive controls can be used to mitigate the occurrence of an action for continuing or taking place at all (e.g. an access list that governs who may read or modify a file or database, or network and host firewalls that block all but allowable activity). The cloud is a special example of how businesses need to assess and manage risk better [8]. Preventive controls for cloud include risk analysis and decision support tools (for example, as being developed within our Cloud Stewardship Economics and Trust Economics projects, HP Privacy Advisor and Privacy Impact Assessments), policy enforcement (for example, machine readable policies, privacy-enhanced access control and obligations that we are developing within the EnCoRe project), trust assessment (as being developed within our Trust Domains project), obfuscation techniques and identity management.

Detective controls are used to identify the occurrence of a privacy or security risk that goes against the privacy or security policies and procedures (for example, intrusion detection systems, policy-aware transaction logs, language frameworks and reasoning tools). Detective controls for the cloud include audit (which we are addressing within our TrustCloud project), tracking, reporting, and monitoring.

In addition, there are corrective controls (e.g. an incident management plan, dispute resolution), which are used to fix an undesired result that has already occurred.

These controls complement each other: a combination of these would ideally be required in order to provide accountability.

Provision of accountability would not just be via procedural means, especially for cloud, which is such an automated and dynamic environment: technology can play an important role in enhancing the solution – by enforcing policies, providing decision support, assurance, security, etc.

Procedural measures for accountability include determining the capabilities of CSPs before selection, negotiating contracts and Service Level Agreements (SLAs), restricting the transfer of confidential data to CSPs and buying insurance. Organisations should also appoint a data protection officer, regularly perform privacy impact assessments on new products and services, and put mechanisms in place to allow quick response to data subject access and deletion requests.

Technical measures for accountability can include encryption for data security mitigation, privacy infomediaries and agents to help increase trust. We also need to be able to rely on infrastructure to maintain appropriate separations, enforce policy and report information accurately. At HP Labs we are investigating how to build and exploit trusted virtualized platforms with precisely these properties. Another mechanism that HP Labs is researching at the moment is the use of sticky policies, where machine readable policies (defining allowed usage and associated obligations) are attached to data within the cloud and travel with it. Other mechanisms that we are currently researching include risk

assessment, decision support, obfuscation in the cloud and policy translation from higher level policies to machine readable policies that are enforced and audited.

We don't have the space here to describe all this work so let's just briefly consider two examples of our research.

First, in the Cloud Stewardship Economics project we are defining mathematical and economic models of the cloud eco-system and the different choices cloud stakeholders face. The goal is to help cloud consumers, providers, regulators and other stakeholders explore and predict the consequences of different policies, assurance mechanisms or even ways of regulating accountability. This can facilitate consumer choice, and as chains of providers become more complex, the models can highlight how and why evidence sharing is likely to provide necessary assurance.

Second, we are working to achieve accountability using contractual assurances along the service provision chain from the CSPs to 'accountable' organisations, enhanced on the technical side by enforcement of corresponding machine-readable policies propagated with (references to) data through the cloud, integrated risk assessment, assurance and audit. By these means the accountable organisations can ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs.

In addition to such research, at HP we have already taken a number of different measures - both procedural and technical – to become an accountable organization in the sense described above. One example is that in Labs we have worked with HP Privacy Office to develop an internal tool called the HP Privacy Advisor that takes employees through a series of dynamically-generated contextual questions and outputs the risks for privacy compliance in any new product, service or program. It encodes our privacy rulebook and other external sources and provides privacy by design guidance. There is an associated workflow with privacy managers to ensure that suggested actions mitigating these risks are addressed.

Moving Forwards

Current regulatory structure places too much emphasis on recovering and not enough on trying to get organizations to proactively reduce privacy and security risks. New data governance models for accountability can provide a basis for providing data protection when cloud computing is used. Accountability is becoming more integrated into our self regulatory programs as well as future privacy and data protection frameworks globally. If CSPs do not think beyond mere compliance and demonstrate capacity for accountability then there is a good chance that regulation may develop that will be difficult to follow and that may stifle innovation, or there could be a backlash from data subjects.

It is an upcoming challenge to strengthen this approach and make it more workable by developing intelligent ways in which accountability and information stewardship can be provided. This goes beyond traditional approaches to protect data (such as the 'CIA' model), in that it includes complying with and upholding values, obligations, and enhancing trust. HP is actively working in this area to produce practical solutions, both on policy (HP Privacy Office) and the technical side (HP Labs).

At present we are just starting to see some technical work emerging from other parties in this area, too. The Cloud Security Alliance (CSA) - a non-profit organization formed to promote the use of best practices for providing security assurance within cloud computing – has a Governance, Risk Management and Compliance (GRC) stack that includes two very relevant activities: CloudAudit, which aims to provide a technical foundation to enable transparency and trust in private and public cloud systems, and the Trusted Cloud Initiative, which is working towards certification of 'trusted clouds'. HyTrust Appliance is a hypervisor consolidated log report and policy enforcement tool that logs from a system perspective. CSIRO has produced a prototype in which CSPs are made accountable for faulty services. CSC is developing a CloudTrust protocol that can be used to promote the transparency of CSPs.

At HP Labs, our broader vision is to deliver seamless, secure, context-aware experiences for a connected world. The richness, choice and convenience of how we interact with our devices and a pervasive computing environment will be enhanced. At the same time, we want this to be safe and ultimately controlled by end users. We've been introducing and will continue to research new innovative techniques to uphold HP's ethics and values internally and demonstrate this to our stakeholders and customers.

References

1. R. Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing". World Privacy Forum, 2009.
2. ENISA, *Cloud Computing: Benefits, risks and recommendations for information security*, ed. D. Catteddu and G. Hogben, November 2009.
3. Cloud Security Alliance, "Top Threats to Cloud Computing", v1.0, March 2010.
4. Galway Project, "Galway Project Plenary session Introduction" April 28th, 2009, p 5.
5. D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler and G.J. Sussman, "Information Accountability", *Communications of the ACM,* vol 51, issue 6, June 2008.
6. S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud", *Proc. 1st CloudCom 2009*, ed. M.G. Jaatun, G. Zhao, C. Rong, Beijing, Springer LNCS 5931, December 2009, pp. 131-144.
7. D. Pym and M. Sadler, "Information Stewardship in Cloud Computing", International Journal of Service Science, Management, Engineering and Technology, 1(1), January-March 2010, pp. 50-67.
8. A. Baldwin and S. Shiu, "Managing Digital Risk: Trends, issues and implications for business", Lloyds 360 Risk Insight, 2010.