Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on, pp.1001-1006, 15-18 Dec. 2014, http://dx.doi.org/10.1109/CloudCom.2014.123 - Expanded journal version available at https://jaatun.no/papers/2016/strongaccountability-journal.pdf

Towards Strong Accountability for Cloud Service Providers

Martin Gilje Jaatun
SINTEF ICT
Trondheim, Norway

Siani Pearson and Frédéric Gittler
HP Labs
Bristol, UK

Ronald Leenes
Tilburg University
The Netherlands

***Abstract*—In order to be an accountable organisation, Cloud Providers need to commit to being responsible stewards of other people's information. This implies demonstrating both willingness and capacity for such stewardship. This paper outlines the fundamental requirements that must be met by accountable organisations, and sketches what kind of tools, mechanisms and guidelines support this in practice.**

***Keywords*—Cloud computing, accountability, security, privacy**

I. Introduction

Cloud Providers have some characteristics that set them apart from many traditional service providers. They offer generic services, where things generally are not custom made. There are also very specific boundaries of concern, depending on the offered service model. 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*.

Another key feature of the Cloud is ubiquity; 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 any single customer. Ease of use is another factor; a standard framework will make the Cloud more natural to 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 I for a brief summary of some Cloud-specific features and related challenges, as identified by Pearson [1]). In general, security concerns are often cited as the most prominent reason for not using cloud computing [2]. At the same time, customers of cloud users, especially end-users, frequently do not understand the need to control access to personal information [3]. 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 risk, and yet have inadequate means to address it [4]. In order to make the Cloud a viable alternative for applications with more stringent security and privacy requirements, accountability of the service providers is key.

To be able 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) [5].

Suppliers within the cloud eco-system need to be able to differentiate themselves in what ultimately is a commodity market, and being able to offer accountability as part of the service provision will represent a competitive edge for service providers catering to discerning cloud customers [6]. This will also be tantamount to extending the cloud market, expanding the definition of "what is it possible to do in the Cloud".

TABLE I: Cloud Computing Features and Related Issues [1]

Cloud Feature	Related 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

II. 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, with cloud as a significant example; the initial focus is on personal data (and therefore, accountability will be understood in the data protection context). However, we will extend beyond scenarios involving personal data, also taking into account situations in which there is an obligation to some person to keep that 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 Accountability for Cloud (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.

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.

III. Requirements

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, which in brief entail that it:

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

Basically the first three bullets describe the standard cybernetic loop (define, monitor, correct) [7][1] as well as the preventive, detective and corrective mechanisms discussed above. This also aligns well with the outcomes of the CIPL Galway [9] and Paris [10] 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 [11], but may extend to types of confidential information that do not involve personal data.
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, but extend those to include all elements that are relevant for customers to make informed choices about the organisation's offering and that allow checking compliance later on (in the monitoring stage) and will also be based on business considerations related to the service provider's services. Policies hence have external (e.g., the law, social norms) and internal (business objectives) sources that are the relevant ones for the given context.
3) **An accountable organisation must monitor its data practices.**
   An accountable organisation outlines how it processes data and has to be able to prove 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).
4) **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 effects of the violation need to be addressed. Errors need to be corrected, and incidents need to be handled. Second, the causes of the violation need to be addressed. 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. 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). In connection with the latter, damages may need to be compensated (financially or otherwise).
5) **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

[1] Or the plan, check, and act components of Deming's circle of continuous improvement [8].

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 evidence that the operational environment is satisfying the policies (cf. point 3 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 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 requisite information about the service provision and remediation.

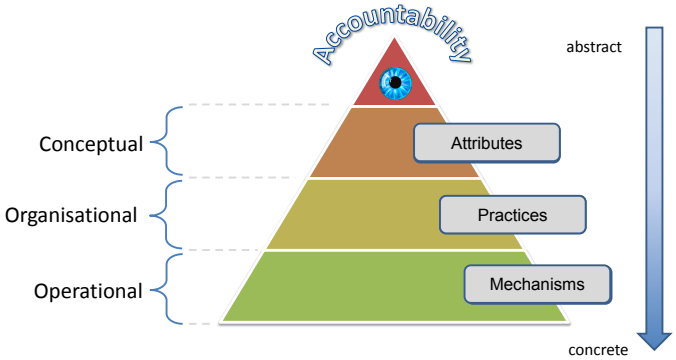

Fig. 1: A Conceptual Framework for Accountability

IV. Conceptual Model

We define accountability [12] as:

> Accountability for an organisation 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 conceptual accountability model (see Fig. 1) elaborates on this definition 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 practices)
- *Accountability mechanisms:* diverse processes, non-technical mechanisms and tools that support accountability practices (that is, accountability practices use them).

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.[2]

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.

To support and implement the main accountability attributes, we have developed a 'toolkit' that forms the bottom layer in Fig. 1 and from which organizations can select as appropriate. The toolkit contains *extensions of existing business processes* like auditing, risk assessment and the provision of a

[2]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.

trustworthy account, *non-technical mechanisms* like formation of appropriate organizational policies, remediation procedures in complex environments, contracts, certification procedures, and so on. Or they 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 usage 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).

V. A Sketch of an Accountability Toolkit

The envisioned tools can be divided in four broad categories corresponding with the objectives in Section **??** : 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 A4C project.

A. 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 (Data Protection Impact Assessment tool (DPIAT)). This tool, 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. An additional tool allows customers of cloud services to express their privacy and security preferences based on the type of data that will be involved and that matches cloud service offerings with these preferences (i.e. the Cloud Offerings Advisory Tool (COAT)). This tool supplements existing cloud brokerage tools that focus on price and performance by focusing on the degree of accountability offered.

B. 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 EU Cloud Accountability (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)). 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). The Data Track tool is designed to facilitate this kind of transparency.

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 [6].

C. Objective 3 – Compliance

Compliance of behaviour with the norms and policies governing the data handling can partly be enforced by technical tools. The A-PPL-Engine is an example here. But also continuous monitoring by system plug-ins that monitor changes in the system are being developed (for instance monitoring configuration files (such as httpd.conf)in relation to selected policies). These tools contribute to a proactive approach to compliance monitoring. 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.

Non compliance and incidents 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 redress. An Incident Response tool is being developed for this purpose.

D. 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 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.

We should also ensure "democratic accountability". Cloud computing does not only affect customers and end-users, but society at large. Transparency should therefore also be aimed at the general public and the regulator. This contributes to the maintenance of ethical standards, rather that stimulating a race to the bottom (of cost and privacy protection).

VI. Discussion

Accountability is a difficult concept to define, and many European languages even lack a word for it. Numerous definitions of accountability exist in different domains (such as public policy, financial sector or enterprise operations) and each focuses on slightly different, context specific, aspects. Hence there is no consensus on a single definition. The definition used in this paper is quite close to the one used by the Galway project [9]:

> An accountability-based approach to data protection [...] requires 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.

The concept of accountability in itself pre-dates the computing industry; Webster's 1828 dictionary [13] 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.

We find that both meanings actually harmonize well with our definition. Ten years ago, Lampson [14] listed accountability as one of the three core objectives of having a security policy, alongside usage control and availability. It is thus surprising that accountability has had such a little impact on the Cloud services that are currently on offer.

We have placed our notion of accountability in the context of privacy and security. Privacy should here not be read in Warren & Brandeis' [15] early, and well known, interpretation – 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 [3]. The buck does not stop here. Big data analytics on purchase history and other metadata allow internet retailers and other major players to infer much more about their users than what they are volunteering [16]. In some cases, this allows a service provider to identify individual users even when they are using the service anonymously. Privacy, in the Warren/Brandeis interpretation certainly seems dead.

A more modern interpretation of privacy, however, stems from Westin's [17] informational privacy – a right to control one's personal data. This interpretation has found its way in, for instance, the European Data Protection Directive. 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"[3] as exemplified by CNIL's recent fining of Google – 150 000 euros is hardly something Google will lose sleep over [18]. However, current plans by regulators across the world (e.g., in the upcoming EU General Data Protection Regulation (GDPR) and also in similar legislation in the US) are to substantially increase penalties for non-compliance and to punish organisations that are not accountable, so it remains to be seen if this will change in the near future.

If indeed the EU GDPR places more emphasis on compliance and accountability, there will be a strong regulatory push towards stronger accountability. 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 of things going wrong. This may provide a strong selling point. The Snowden revelations have caused ripples in people's and organisations' trust in information services. 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 V will need to be complemented by other security tools to make security and privacy stronger, for instance by enforcing confidentiality and anonymity where desired.

While we believe that the importance of confidentiality and privacy enhancing technologies [3] will continue to increase in the years to come, we also agree with Weitzner et al. [19] 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 [20] 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. [19]

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, and what they use it for.

We believe that much can be achieved by the providers taking a more conscious approach to data stewardship. They need to be upfront about what kind of data they collect and store, what they use it for, and how it is shared with others.

VII. Conclusion

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 V 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

[3] 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

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 [1], and that a certification scheme inevitably will emerge, much like we see for the Payment Card Industry Data Security Standard (PCI-DSS) [21]. 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, Maartje Niezen and Alain Pannetrat.

REFERENCES

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

[2] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 39, no. 1, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790612000870

[3] M. G. Jaatun, Å. A. Nyre, I. A. Tøndel, and K. Bernsmed, "Privacy Enhancing Technologies for Information Control," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, G. M. Yee, Ed., 2012.

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

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

[6] J. Prüfer, "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, Dec 2013, pp. 33–38.

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

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

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

[10] ——, "Demonstrating and Measuring Accountability - A Discussion Document - Accountability Phase II (the Paris Project)," Centre for Information Policy Leadership, October 2010.

[11] European Parliament, "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." pp. 31–50, 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

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

[13] N. Webster, *American Dictionary of the English Language*, 1828. [Online]. Available: http://webstersdictionary1828.com/

[14] B. W. Lampson, "Computer security in the real world," *Computer*, vol. 37, no. 6, pp. 37–46, 2004.

[15] S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harvard Law Review*, pp. 193–220, 1890.

[16] J. Podesta, P. Pritzker, E. J. Moniz, J. Holdren, and J. Zients, "Big data: Seizing opportunities, preserving values," Executive Office of the President, May 2014.

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

[18] (2014) The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc. [Online]. Available: http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/

[19] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information accountability," *Communications of the ACM*, vol. 51, no. 6, 2008. [Online]. Available: http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf

[20] F. B. Schneider, "Accountability for perfection," *IEEE Security & Privacy*, vol. 7, no. 2, pp. 3–4, 2009.

[21] (2013) Payment Card Industry Data Security Standard. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0