The Ethics of Cloud Computing

A Conceptual Review

Job Timmermans
Technical University of Delft
Delft, The Netherlands
j.f.c.timmermans@tudelft.nl

Veikko Ikonen
VTT
Tampere, Finland
Veikko.Ikonen@vtt.fi

Bernd Carsten Stahl
Centre for Computing and Social Responsibility
De Montfort University
Leicester, UK
bstahl@dmu.ac.uk

Engin Bozdag
Technical University of Delft
Delft, The Netherlands
bozdag@gmail.com

***Abstract*—Cloud computing can raise ethical issues. In many cases these will depend on particular applications and circumstances. The present paper sets out to identify ethical issues of cloud computing that arise from the fundamental nature of the technology rather than any specific circumstances. The paper describes how these general features were identified, how ethical issues arising from them were collected and it concludes by discussing means of addressing them.**

Keywords: ethics, social impact, cloud computing, emerging technology

I. INTRODUCTION

Cloud computing can be described as a current buzz word and research fashion. It is gaining prominence in commercial mainstream computing and even among private end users who are not among early adopters. It is viewed as one of the fastest growing segments in the computing industry that will take over and affect many or most aspects of computing.

Just following this hype it is easy to see that cloud computing can lead to numerous ethical issues. The most obvious one is privacy which can arise as a problem when users store personal data in clouds and lose control of who has which access and usage rights. Similar issues can occur with regards to intellectual property which can become dispersed among different jurisdictions leading to all sorts of legal and ethical questions.

There is thus good reason to believe that cloud computing warrants ethical analysis. A much more difficult question is how to do this ethical analysis. Are there pervasive ethical issues in cloud computing or are they all context relative? How can we know which issues count as ethical and how are they to be evaluated? These are questions to which there currently is no generally agreed answer. The present sets out to give a high level answer to them. It provides a general description of cloud computing. The defining features of cloud computing are first presented, and then used as a starting point for an ethical analysis of the technology *per se*. The paper concludes by outlining possible ways of addressing these issues.

II. CLOUD COMPUTING

While cloud computing is a technical and social reality, it is also still an emerging technology. We do not yet know what it will be used for in the future and which social, ethical, or legal consequences these uses will have. At the same time it is advisable not to wait until unexpected and undesirable effects happen. Early recognition of ethical and related issues can save time and money to be spent later in overcoming them. It can support user acceptance and promote beneficial aspects of the technology.

This paper aims to provide an early and general insight into ethical issues of cloud computing. In order to do this, it must start with a clear understanding of the concept of cloud computing and the features of the technology that may give rise to ethical questions. This is achieved by first briefly reviewing the history of the term and defining the overarching characteristics and features of the technology. These are identified and underpinned by the literature on cloud computing. This will then provide the basis for an ethical analysis.

A. History and definition

The history of cloud computing as a concept that would deliver computing resources to different locations through a global network was originally introduced in the sixties. J.C.R Licklider's idea of an "intergalactic computer network" seems to be quite similar to what we are now calling cloud computing. Licklider was responsible for enabling the development of ARPANET. Another pioneer of cloud computing is John McCarthy who envisioned in the beginning of 60s that computation may someday be organized as a public utility like water or electricity. Cloud computing has developed since the sixties and since the offer of a significant bandwidth in the nineties; it could be developed to serve the masses. The evolution of cloud computing has gone through many phases such as gird and utility computing, application service provision (ASP), and Software as a Service (SaaS). (Mohammed 2009, Dikaiakos et al 2009)

One can state, that Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers. It basically means that applications are delivered as services over the Internet as well as to the actual cloud infrastructure. (Dikaiakos et al 2009, Gartner 2009) From user point of view it means, that the user can access his/her files, data, programs and other services from a Web browser via the Internet that are hosted by other service providers. (Won 2009) On the other hand you can also look at cloud computing from more general view and define it as a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies. As enterprises seek to consume their IT services in the most cost-effective way, interest is growing in drawing a broad range of services (for example, computational power, storage and business applications) from the "cloud," rather than from on-premises equipment. The levels of hype around cloud computing in the IT industry are deafening, with every vendor expounding its cloud strategy and variations, such as private cloud computing and hybrid approaches, compounding the hype. "(Gartner 2009)

Gmail, Google Docs, Twitter, Facebook are all cloud applications. Major IT providers such as Google, Microsoft, Sun and IBM are all offering cloud services. Several software companies such as Salesforce[1] offer their software only via the cloud. Cloud applications range from webmail[2], nomadic business organizations[3] to medical practice/patient information sharing[4]. Government agencies also recently started to use cloud applications[5].

B. *Defining Features*

While cloud computing is expanding rapidly and used by a great many individuals and organizations, ethical issues related to this technology are not being widely discussed or considered. The variety of technologies involved in cloud computing, and the hype around it causes a "conceptual muddle" (Moor 2006 and Vaquero et al. 2009), leading to a vague definition of cloud computing[6]. In order to have a more focused ethical analysis, in this subsection we list the defining features of this technology.

Looking at various cloud application and the literature on the topic, one can distill a number of defining features of the technology. This list does not claim comprehensiveness and to reflect all possible uses and all relevant aspects of cloud computing. What it aims to do is provide a high level decontextualised view of the nature of technology that will be subjected to an ethical analysis in the next section. The main relevant features we identified are these:

- **Resource/storage virtualization**
- **Scalability and elasticity**
- **Efficiency of resource sharing**
- **Usage optimizing/optimized by usage**
- **Ease of usage**
- **Fast information sharing, delivery and control**
- **Accessibility**
- **Anonymity**

The resources and services are delivered to users and/or organizations via Internet from resource clouds where almost all information and tools are preserved. Resources can be added or removed based on the changes in needs. Resources from the service provider are thought to be used with maximum efficiency and serve multiple needs for multiple parties at the same time, as they are *shared* with other consumers or organizations. People or organizations might not know where the information or services are coming from or where their information is preserved. It is assumed that all the services will be available via Internet with various devices. The ease of use of cloud services is emphasized. A defining feature of cloud computing is also, that it can be metered by use enabling then resource optimization for particular usages.

An alternative way of summarizing the main features of cloud computing is the following: Cloud computing (1) uses internet technologies to offer (2) scalable and (3) elastic (4) services that can be (5) metered by use and are (6) more cost effective partially due to (7) multi-tenancy efficiency benefits. Data is stored (8) device and location independent making storage potentially more (9) reliable and (10) secure. Moreover (11) maintenance and (12) security are outsourced to service providers increasing their efficiency and effectively through specialization and centralization.

III. ETHICAL ANALYSIS OF CLOUD COMPUTING

An ethical analysis would be well served by starting with definition of the concept of ethics. However, ethics is a very complicated term with a large number of meanings and

---

[1] http://www.salesforce.com

[2] For instance, Gmail: http://www.gmail.com

[3] For instance, The Think Trust project, http://www.think-trust.eu/

[4] See Andriole and Khorasani 2010 for implications of cloud computing in this field.

[5] The City of Los Angeles uses Google Apps for e-mail and other applications. The White House recently launched www.apps.gov to encourage federal agencies to use cloud services.

[6] Users misunderstand or perceive the term cloud computing differently. For instance, Dutch state secretary Bijleveld defines cloud computing as follows: "…And then there is cloud-computing: cooperating and sharing information through the internet. (…) it is unfit for private or confidential information and not suitable for official business, for local or national government." See http://www.minbzk.nl/actueel/toespraken/@122958/toespraak-van

consequences. The present paper is not in a position nor meant to be reviewing this. Very briefly, the stance taken here is one of descriptive ethics. That means that the authors of this paper did not endeavor to undertake their own ethical analysis, which would have required them to offer a philosophical foundation and justification and then to apply some ethical principle or theory to cloud computing. Instead, the idea was to review the relevant literature, namely the literature on ethics and ICT with a view to identifying either discussions of cloud computing per se or discussions of the defining features or aspects of these with a view to gaining a broader overview of what is perceived and described to be ethically problematic about cloud computing. The details of this approach and a more fine-grained justification can be found in Stahl et al. (2010).

Not surprisingly, this review of the ICT ethics literature showed that the features of cloud computing as outlined in the previous section give rise to several ethical issues. To keep the discussion focused, only those issues are addressed here that are typical for cloud computing. Issues that overlap those of other emerging technologies or raise wider concerns beyond cloud computing are left out of the analysis.

The review of the literature on ICT ethics showed that cloud computing as such isn't addressed directly in the established outlets of this field of study. The technology is therefore dealt with in an indirect fashion. Issues are analyzed that came to the forefront in non-ethical resources on cloud computing partially stemming from the technology description.

In essence cloud computing amounts to three developments that are relevant to an ethical analysis:

1) The shifting of control from technology users to the third parties servicing the cloud due to outsourcing and off shoring of ICT functionality to the cloud.

2) The storage of data in multiple physical locations across many servers around the world possibly owned and administrated by many different organizations.

3) The interconnection of multiple services across the cloud. At different levels functionality of different providers is connected to provide a specific service to an end-user.

These will play a central role in the following discussion of individual ethical issues of cloud computing.

A. *Control*

Cloud computing entails the outsourcing or off shoring of ICT tasks to third party service providers. Any information that used to be stored locally is stored in the cloud. The user thus places his computation and data on machines he cannot directly control. Thereby, to a large extend customers or users of a cloud computer service relinquish control over computation and data (Haeberlen 2010, Kandukuri 2009, Grimes 2009).

The loss of (direct) control can become problematic if something goes wrong. Among risks associated with cloud computing are unauthorized access, data corruption, infrastructure failure, or unavailability/outing (Paquette 2010). In case something goes wrong it can be difficult to discern who has caused the problem, and, in the absence of solid evidence, it is nearly impossible for the parties involved to hold each other responsible for the problem if a dispute arises (Haeberlen 2010).

Contributing to this, is the fact that as a result of cloud computing the border between what is part of one's own IT infrastructure and what lies outside it is blurred. Systems can span the boundaries of multiple parties and cross the security perimeters that these parties have put in place (Pieters 2009). This process is called de-perimeterisation: "the disappearing of boundaries between systems and organisations, which are becoming connected and fragmented at the same time" (Pieters 2009, p.2). As a result of de-perimeterisation not only the border of the organizations IT infrastructure blurs, also the border of the organization's accountability becomes less clear.

In a networked organizational and technological structure it becomes increasingly difficult to ascribe consequences of actions to a single person or organization.

B. *Problem of many hands*

Moreover, since responsibilities are divided between customer and provider of the service, neither of them is in a good position to address these problems (Haeberlen 2010). This typically may lead to what is referred to in ethical literature as 'the problem of many hands'. This occurs when "in a complex chain of events or systems, many people will have had a share in an action that leads to undesirable consequences. As such many people will also have had the opportunity to prevent these consequences, and therefore no-one can be held responsible." (Pieters 2009, p.2)

In cloud computing a specific service delivered to a user depends on another system, which in turn depends on other systems as well. A cloud service to the end-users for example can be built on a framework serviced in the cloud by another company. Cloud computing typically makes use a service-oriented architecture (SOA) where all functionality consists of services which can be aggregated into larger applications performing functions to end-users (Pieters 2009). The complex structure of cloud services can make it difficult to determine who is responsible in case something undesirable happens.

C. *Self-determination*

Ceding control to the Cloud provider also raises the question of information self-determination. Informational self-determination refers to the right or ability of individuals to exercise personal control over the collection, use and disclosure of their personal data by others (Cavoukian 2008).

In a world of ubiquitous and unlimited data sharing and storage among organizations self-determination is challenged. This not only raises privacy issues - discussed in depth below- but also puts at stake the confidence and trust of in today's evolving information society (Cavoukian 2008). Organizations offering cloud computing services must accommodate the interests of their users/customers. They can do this by: "by being open and accountable about their data management practices, by seeking informed consent from individuals, and by providing them with credible access and redress mechanisms." (Cavoukian 2008, p.90)

D. *Accountability*

Data, especially personal data, stored in the cloud should be managed properly. Accountability provides a promising approach to empower users to ensure this is being done. Users of an accountable cloud would be able to check whether the cloud is performing as agreed (Haeberlen 2010). For the provision of accountability transparency -adequate information about how data is handled within the cloud- and a clear allocation of responsibility are key elements (Pearson 2009). Together with recorded evidence, these elements could be used to decide who is responsible whenever a problem occurs or dispute arises.

Since accountability requires detailed records of actions by its users in the cloud, there can be a tension between privacy and accountability (Pearson 2009). It is therefore important to consider what is being recorded, and who the record is made available to.

Moreover, as argued earlier, in a de-perimeterised world not only the border of the organizations IT infrastructure blurs, also the border of the organization's accountability becomes less clear (Pieters 2009).

E. *Ownership*

The off shoring of data also raises the question of who owns the data a user stores in the cloud and what can the providers of cloud services do with this information (Murley 2009, Grimes 2009). Free software advocate Richard Stallman called cloud computing a 'trap' that will take control and freedom away from users and force them into an unnecessary dependency (Grimes 2009).

Besides data actively stored in the cloud by users, the cloud also generates data itself for different purposes: to provide accountability (as seen above), to improve the services provided, or other reasons such as performance or security. Bit by bit, megabyte by megabyte, terabyte by terabyte our digital interactions and tracks are being gathered together thanks to the use of unique identifiers and sophisticated matching algorithms (Cavoukian 2008). This leaves a trail of often extraordinarily detailed personal information that, if not properly protected, may be exploited and abused (Cavoukian 2008, Picker 2008). To date, only few limitations in how they use the information are in place (Picker 2008). In addition once this information is located in one or more databases "in the cloud", it may be accessed and used in ways that individuals never envisioned or intended, and with little oversight.

Although identity-based systems will provide us many benefits, new risks and threats are emerging as well. "Identity fraud and theft are the diseases of the Information Age made possible by the surfeit of personal data in circulation, along with new forms of discrimination and social engineering made possible by asymmetries of data, information and knowledge" (Cavoukian 2008, p.90).

Also it has been argued that information stored with a third party like a cloud computing provider has weaker privacy protection than when the information remains only in the possession of the person. Government agencies and private litigants may be able to obtain information from a third party more easily than from the original owner or creator of the content (Gellman 2009)

Questions about ownership also do arise in relation to infringements on copyrights. "By giving customers access to almost unlimited computing power and storage, Cloud services could make it even easier to share copyrighted material over the Internet." (Nelson 2009).

F. *Function creep*

Another threat to data stored in the cloud is the so-called function creep: data collected for a specific purpose, over time may become used for other (unanticipated, unwanted) purposes. For example a database with biometric data of citizens may be designed for authentication purposes but may then turn out to be very helpful for crime investigations (Pieters 2009). In a world of cloud computing, with its relinquished control and reduced sight on what data is being used for, function creep may become serious danger.

G. *Monopoly & lock-in*

The position of users may further be in jeopardy because of the tendencies for power to centralize in cloud computing. With two of the defining features being economics of scale and network effects, we "may see a future with only a handful of cloud computing providers in which the world will do their computing on." (Grimes 2009). If only a handful of companies are able to achieve a dominant position in the market for cloud services, this might lead abuse or could be harmful otherwise to the interests of the users (Nelson 2009). When the uses of resources are dictated by corporations autonomy of users might be at stake. Therefore, analogous to other ICT markets as desktop software and online advertisement, concerns of the potential for cloud computing monopolies have to be taken into account.

Risks of unwanted dependency on cloud service providers are reinforced by possible vendor lock-ins (ENISA 2009). At the moment there is " little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability" (ENISA 2009). This can make it hard for users to migrate from one provider to another or migrate data and services back to an in-house IT environment thereby introducing a dependency on a particular cloud provider for service provision.

H. *Privacy*

As stated above, many companies providing cloud services collect terabytes of data, much of it sensitive personal information, which is then stored in data centers in countries around the world. As a result a critical factor affecting the development and acceptance of Cloud computing therefore will be how these companies, and the countries in which they operate, address privacy issues (Nelson 2009). Concerns on privacy-matters are widely acknowledged by governments, researchers, users and providers of cloud services alike.

Whenever ethical issues arise concerning information about persons they are typically cast in terms of *privacy*."(Van den Hoven, 2008). Although there is consensus that privacy is important, the concept remains hard to explicate or pin down. In general it aims to constrain access to certain types of personal data and prevent persons to acquire and use information about other persons. Since there is much debate on the moral justification of a right to privacy, the actual reach of privacy-protection remains vague (Van den Hoven, 2008).

Especially in the case of personal data stored in the cloud, vagueness about privacy can be potentially harmful. As data is no longer stored locally, control over the data is shifted to the service providers. Consumers then need to trust the cloud provider that certain personal information will not be exposed. But not only is it likely that different server providers have different opinions on privacy, to the costumers it will not always be clear with which services provider he/she is dealing. In the cloud different services increasingly become intertwined: a hosted application of one company for instance can be built on a development/deployment framework of another. Both reasons imply that to consumers it will not always be clear what they can expect from service providers in the cloud concerning privacy.

I. Privacy across (cultural) borders

Different opinions on privacy are further enhanced by cultural differences. Services and data-storage can be located in any part of the world. Users of cloud services therefore will have to deal with the different cultures predominating specific locations.

Capurro (2005) argues that privacy is affected by cultural differences. Opposed to the Western orientation Eastern countries for example put more emphasis on the concept of community and "give privacy at least partly a negative connotation."(p.46) "In a very general way we can say that the concept of privacy in the West is oriented towards the individual, while Eastern countries – and also other cultures like the African ones, for instance – stress the concept of community and give privacy at least partly a negative connotation."(p.46) This leads to an ambivalent attitude towards the question of privacy with regard to the internet. So, although different cultures at least share a minimal sense of privacy, the lack of a internationally accepted rich sense stands in the way of robust privacy protection on the internet (Moor 2004).

Charles Ess partly concurs to the line of reasoning of Capurro. On the one hand, Ess (2008) admits that there are irreducible differences between diverse cultures. These differences may lead to deep conflicts and divergences in global ethics, countering the optimistic view that a global ethics – and thus the development of a global account of privacy. But this doesn't mean that there is no hope for intercultural practices like cloud computing with respect to overcoming and dealing with ethical differences (Moor 2004, Ess 2008).

On the other hand Ess (2008) demonstrates that convergences do take place that produce norms and values as legitimate for more than a single culture or national tradition. By tracing out pluralistic middle grounds both relativism and dogmatism can be avoided in this process. Indeed globalization itself can play a part stimulating the interaction between individuals belonging to different communities and consequently an interchange of moral norms and values contributing to a global consensus on ICT-ethics (Collste 2007). In China for instance an expansion of the scope of respect for privacy is discerned stemming from globalization, incorporating both traditional Chinese values and Western values (Yao-Huai 2005).

Cloud computing not only provides an urgency for a dialogue between different cultures it can also contribute by providing the all-encompassing infrastructure necessary to exchange, collaborate and communicate across cultural borders.

J. Cultural imperialism and dealing with diversity

We should be wary of cultural imperialism though. Especially since large corporations that are and will most likely be dominating the cloud mostly stem from Western cultures predominantly the US. By implementing Western values one-sidedly into cloud applications, frameworks and its regulations, cloud computing may lead to increasing cultural homogenization, suppressing local cultures (Ess 2008). Actors involved in Cloud computing should not only do justice to local differences but also can play a part in overcoming those differences. Not by imposing values but by bridging cultures from a pluralistic perspective. Ethicists can play an important role in reaching the middle ground and bridging the gap between ethical theory and practical application (Moor 2005).

That's all the more true now 'the Internet and the Web come to connect more and more people and cultures outside their origins in the United States, these domains reflect an extensive diversity, if not cacophony, of cultural identities, traditions, voices, views, and practices'(Ess 2008). As the web, fueled by cloud computing truly is going global, dealing with diversity ethically becomes even more urgent.

IV. WAYS OF DEALING WITH ETHICS OF CLOUD COMPUTING

The discussion of ethical issues of cloud computing contains some of the obvious candidates such as privacy that anybody interested in cloud computing might have foreseen. Others, such as cultural imperialism or issues of accountability may be less obvious and indicate that the present paper makes a relevant contribution to knowledge.

It is important to underline that the paper does not claim to cover all ethical issues of cloud computing. In real life contexts new problems are likely to arise that an abstract conceptualization cannot capture. However, the abstract list of ethical issues can serve to inform, vendors, users or designers of such systems to develop awareness of ethical questions and be proactive in assessing their role in specific implementations and uses.

This leads to the question what can be done to be proactive about ethics of cloud computing. This is an exceedingly difficult question as it touches on some of the core issues of moral philosophy. How can moral behavior be recognized and how can it be implemented? These questions have fascinated and entertained generations of philosophers and we will not give final answers to them. We can nevertheless speculate about some possible ways forward.

A. Precautionary principle

As an approach to deal with risk and responsibility issues in cloud computing Pieters and Van Cleeff (2009) suggest the precautionary principle. They argue that due a de-perimetersition of organizations ethics of consequences no longer satisfies “as consequences may not be foreseeable, their desirability may not be unambiguously assessable, and they cannot be directly ascribed to actions of a single person or a single organisation.” (Pieters 2009, p.13)

The precautionary principle sets out to prevent harm from unknown consequences without hampering progress and innovation altogether. It states that one should refrain from actions in the face of scientific uncertainties about serious or irreversible harm. Furthermore, the burden of proof for assuring the safety of an action falls on those who propose it (Pieters 2009).

Many effects and (unwanted) consequences of cloud computing cannot yet be identified. This does not mean its development and implementation should be aborted altogether. Instead the precautionary principle urges the parties involved to anticipate consequences that are not foreseeable. The burden of proof is placed on them. Moreover, they may never use uncertainty to refrain from designing and providing services that invite moral sound use and inhibit undesirable or controversial actions (Pieters 2009).

B. ICT Governance

Many of the responses to ethics in technology are related to governance. Governance in the political meaning of the word refers to the way in which a country is governed. However, governance in a wider sense can stand for the "manner in which something is governed or regulated; method of management, system of regulations." (OED online, accessed 28.06.2010).

All technology, including ICT, is subject to a range of governance arrangements. These include technical standardizations, professional procedures and informal agreements as much as national and international law and regulations.

With this concept of governance, one can ask how ethics can be integrated into technology development and use. Depending on the type of technology and the context of its use, some governance arrangements are more conducive to the inclusion of ethics than others. In a regulated funding regime, for example, explicit attention to ethics can be required. An example is that of EU research funding in the current 7th Framework Programme which requires all proposals to pay explicit attention to ethical issues. At the same time, other contexts such as those of private company development are much less subject to ethics-related oversight and governance arrangements are more conducive to organizational goals, such as profit generation.

The question is how ethics can be incorporated into such different structures and processes. The first part of the answer to this question will be to lead to a more general recognition of the relevance of ethics in technology including cloud computing. Only when those actors involved in the different stages of technology development and use agree that ethics is an important issue to consider will they consider principles and governance arrangements that allow them to pay attention to it. The second question then is how to implement processes and structures that allow for ethical sensitivity.

The present paper cannot answer either of these questions. However, it has made a contribution to both. By showing the range of potential ethical issues that arise from the overarching features of cloud computing it has demonstrated that ethics and cloud computing are related. How this relationship is interpreted, for example as a risk to user acceptance or as an independent issue requiring further attention is different matter. In either case the paper should raise awareness and knowledge. The second question, that of implementation, is an even more complex one. The present paper's contribution to this question is that it can serve as an early warning sign that offers individuals and organizations interested in ethics of cloud computing a starting point for further discussion.

In any event, we hope that this paper contributes to a rising awareness of practitioners in cloud computing of the importance of ethics in their work which is a necessary condition of addressing these issues.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 230318.

REFERENCES

[1] K.P. Andriole and R. Khorasani. (2010). Cloud Computing: What Is It and Could It Be Useful? Journal of the American College of Radiology. Volume 7, Issue 4, Pages 252-254 (April 2010)

[2] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali. (2009). Cloud Computing: Distributed Internet Computing for IT and Scientific Research. IEEE Internet Computing, vol. 13, no. 5, pp. 10-13, September/October, 2009.

[3] J. Fenn, M. Raskino and B. Gammage (2009). Hype Cycle for Emerging Technologies. Gartner. (Retrieved 13.6.2010 from: http://www.gartner.com/resources/169700/169747/gartners_hype_cycle_special__169747.pdf)

[4] A. Mohamed (2009, March 27). *A History of Cloud Computing*. Retrieved June 13, 2010, from ComputerWeekly: http://www.computerweekly.com/Articles/2009/03/27/235429/a-history-of-cloud-computing.htm

[5] S. Paquette, P.T. Jaeger, and S.C. Wilson (2010). Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly 27(3), pp. 245 - 253

[6] B. C. Stahl, R. Heersmink, P.G. Goujon, C. Flick, J. van den Hoven, K. Wakunuma, V. Ikkonen and M. Rader (in press): Identifying the Ethics of Emerging Information and Communication Technologies: An Essay on Issues, Concepts and Method International Journal of Technoethics

[7] The Think-Trust project: Think-Trust (FP7-216890) http://www.think-trust.eu/downloads/think-trust-documents/cloud-computing_v0-2/download.html (accessed 8.6.2010)

[8] K. Won (2009) Cloud Computing: Today and Tomorrow. Journal of Object technology. Vol. 8, No. 1, January-February 2009.

[9] J. Van den Hoven (2008). Information Technology, Privacy and the Protection of Personal Data. Information Technology and Moral Philosophy(2008), Jeroen van den Hoven and John Weckert (Eds.). P 301-321

[10] C. Ess.(2008). Culture and Global Networks, Hope for a Global Ethics? In Information Technology and Moral Philosophy(2008), Jeroen van den Hoven and John Weckert (Eds.). P 195-225

[11] R. Capurro (2005). Privacy. An intercultural perspective. In *Ethics and Information Technology* (2005) (7), P 37–47

[12] A. Haeberlen (2010). A case for the accountable cloud. *SIGOPS Oper. Syst. Rev.* 44, 2 (Apr. 2010), 52-57. DOI= http://doi.acm.org/10.1145/1773912.1773926

[13] S. Paquette, P. T. Jaeger and S. C. Wilson (2010). Identifying the security risks associated with governmental use of cloud computing, *Government Information Quarterly*, In Press, Corrected Proof, Available online 13 April 2010, ISSN 0740-624X, DOI: 10.1016/j.giq.2010.01.002.

[14] B. R Kandukuri and A. Rakshit (2009). Cloud Security Issues. In *Proceedings of the 2009 IEEE international Conference on Services Computing* (September 21 - 25, 2009). Symposium on Compiler Construction. IEEE Computer Society, Washington, DC, 517-520. DOI= http://dx.doi.org/10.1109/SCC.2009.84

[15] P. Wolter and A. van Cleeff (2009).The Precautionary Principle in a World of Digital Dependencies. In Computer, vol. 42, no. 6, pp. 50-56, May 2009, doi:10.1109/MC.2009.203

[16] A. Cavoukian (2008). Privacy in the clouds. In Identity in Information Society (1) (2008) p. 89-108

[17] S Pearson and A. Charlesworth (2009) Accountability as a Way Forward for Privacy Protection in the Cloud., In Cloud Computing(2009), M.G. Jaatun, G. Zhao, and C. Rong (Eds.):, p. 131–144

[18] D. Murley (2009). Law Libraries in the Cloud. Law Library Journal, Vol. 101, No. 2 (2009). Available at SSRN: http://ssrn.com/abstract=1335322

[19] J. M. Grimes, P. T. Jaeger and J. Lin (2009) Weathering the Storm: The Policy Implications of Cloud Computing. http://nora.lis.uiuc.edu/images/iConferences/CloudAbstract13109FINAL.pdf (visited 29 April 2010)

[20] R. C. Picker (2008). Competition and Privacy in Web 2.0 and the Cloud. U of Chicago Law & Economics, Olin Working Paper No. 414. Available at SSRN: http://ssrn.com/abstract=1151985

[21] R. Gellman (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum (2009). From: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (Retrieved 27 April 2010)

[22] M. R. Nelson (2009) The Cloud, the Crowd, and Public Policy. Issues in Science and Technology (2009). From: http://www.issues.org/25.4/nelson.html, Retrieved (25 April 2010)

[23] ENISA - The European Network and Information Security Agency (2009) , Cloud Computing , Benefits, risks and recommendations for information security. From: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (15 April 2010)

[24] J. H. Moor, M. Mizutani and J. Dorsey (2004). The internet and Japanese conception of privacy. Ethics and Inf. Technol. 6, 2 (Jun. 2004), 121-128. DOI= http://dx.doi.org/10.1023/B:ETIN.0000047479.12986.42

[25] L. Yao-Huai (2005). Privacy and Data Privacy Issues in Contemporary China. Ethics and Inf. Technol. 7, 1 (Mar. 2005), 7-15. DOI= http://dx.doi.org/10.1007/s10676-005-0456-y

[26] G. Collste (2007). Globalisation, Ict-Ethics And Value Conflicts, In The ETHICOMP Journal (3) (2008)

[27] Gartner (2009). Gartner Special Report, The What, Why and When of Cloud Computing, cited at http://www.cioupdate.com/features/article.php/3827971/The-Five-Attributes-of-Cloud Computing.htm (20 April 2010)

[28] Moor, J. (2006). Why we need better ethics for emerging technologies. Ethics and Information Technology , 111-119.

[29] Vaquero, L. M., Rodero-Meniro, L., Caceres, J., & Lindner, M. (2009). A Break in the Clouds: Towards a Cloud Definition. Computer Communication Review 39 (1) , 50-55.