How to Govern the Cloud?

Characterizing the optimal enforcement institution that supports accountability in cloud computing

Jens Prüfer
Tilburg School of Economics and Management
Tilburg University
Tilburg, The Netherlands
j.prufer@uvt.nl

Abstract— **This paper applies economic governance theory to the cloud computing industry. We analyze which governance institution may be best suited to solve the problems stemming from asymmetric information about the true level of data protection, security, and accountability offered by cloud service providers. We conclude that certification agencies - private, independent organizations which award certificates to cloud service providers meeting certain technical and organizational criteria - are the optimal institution available. Those users with high valuation for accountability will be willing to pay more for the services of certified providers, whereas other users may patronize uncertified providers.**

Keywords— Economic governance, institutions, accountability, associations, certification agencies, cloud computing

I. INTRODUCTION

Whereas cloud computing has been the subject of research in computer science and other hard sciences for years, economists have ignored the field until recently, with few exceptions, which are mostly focused on privacy issues [1], [17]. Today, however, the common wisdom about the potential productivity gains of the cloud is spreading. A recent estimate expects that spending on the cloud by financial-services firms alone will total U$26 billion in 2015 [29]. Moreover, cloud computing has the potential to reduce the fixed costs of entry and production, which could boost the creation of jobs and new firms. This could foster in particular small and medium-sized enterprises and thereby contribute significantly to economic growth all over the world [12].

But there are important impediments to the wide adoption of cloud computing. A key concern is the worry over privacy, security, and data protection. If individual users do not trust Cloud Service Providers (CSPs) to keep their private data private, they will not use cloud technologies up to the level they would do without such concerns. We refer to CSPs as sellers of any kind of cloud computing services [21]. If business users, who may have obligations to treat data of their customers securelyor whose prospects may depend on keeping a few business secrets, worry that data put to the cloud could leak to their competitors or other parties, they may voluntarily forego potential benefits of this technology. The recent revelations about extensive espionage of public intelligence agencies on private computing devices, even if unrelated to cloud computing directly, have increased public awareness of the privacy and data security problems surrounding Internet-based technologies [31]. Related, the policies of several governments, most prominently in the United States, to reserve the right to access data stored by firms registered in their countries under certain circumstances, shatters the trust of users that access to data stored in the cloud is limited to those parties defined by the data owner [28].

As a consequence, both individual and business consumers may underutilize the opportunities inherent in cloud computing technologies [6], which mitigates innovation and economic growth. Creating accountability in the cloud is seen as a solution to users' lack of trust [24], where accountability refers to a situation, where both the CSP and the user "should be able to check whether the cloud is running the service as agreed. If a problem appears, they should be able to determine which of them is responsible, and to prove the presence of the problem to a third party, such as an arbitrator or a judge" [16]. Hence, the concept of accountability also encompasses data protection and security. It can reduce the threats and spur the upside potential of cloud computing.

This paper contributes to creating accountability in cloud computing by characterizing an institution that mitigates the problems identified and helps to increase users' trust in the data security and privacy promises of CSPs. The following research questions aries: How can we increase the level of trustworthy behavior of CSPs with respect to the security and privacy of their clients' data? How can we improve the incentives for CSPs to invest in the security technology and accountable organizational structures necessary to protect their clients' data, even if data storage or another procedure is partly outsourced? Under which circumstances could a cloud user be sure that her data is neither accessed by other private parties nor by any government?

We study these questions by applying an existing classification of contract enforcement institutions [19] and discussing the pros and cons of each of the theoretically available institutions to mitigate the accountability problem in cloud computing.

After outlining the main impediments to establishing accountability in section II, we argue that public regulations and enforcement are inferior mechanisms to private ordering

978-0-7695-5095-4/13 $31.00 © 2013 IEEE
DOI 10.1109/CloudCom.2013.100

when establish accountability in the cloud in section III. In section IV we narrow down the set of feasible enforcement institutions. We argue in section V that the optimal institution for the cloud computing industry is a privately managed nonprofit certification agency with certain characteristics. In section VI we conclude and outline the research agenda following up on this result.

II. Impediments to Establishing Accountability

According to Pearson et al. [23], there are three main goals of developing an accountability framework for cloud computing. First, individual users fear that their privacy concerns are not respected. Business clients are suspicious that their own or their customers' sensitive data are not secured, which may bring them at odds with their duties as data controllers [28]. Moreover, regulators, restricted by national jurisdictional boundaries, are worried about the increasing internationalization of internet-related applications, which diminishes and complicates their propensity to oversee. This process is accelerated by cloud computing.

Second, the international nature of the industry has already confronted businesses with a multitude of legal and regulatory regimes, which are constantly developed further and, as a whole, load large legal and economic liabilities onto CSPs. This increases the explicit and implicit cost of doing business in the cloud and also binds many resources of regulatory agencies.

Third, these problems are amplified because the cloud computing industry is still in an early development stage and is a complex and dynamic business environment. However, the necessary flexible tools for oversight and rules for businesses are not in place, yet.

Consequently, both individual and business consumers underutilize the opportunities inherent in cloud computing technologies. In economic terms, the industry is in a bad equilibrium: a situation where no party has an incentive to change its behavior unless the other parties involved change their behavior, too. Specifically, users do not fully trust the data protection and privacy promises that CSPs commit to in service contracts because of the problems described above. CSPs, on the other hand, cannot credibly convey the information, that their security level is high, to users because most users lack the technical expertise and time necessary to evaluate such information. Therefore, CSPs with high security levels cannot command a price premium, which destroys their incentives to invest in high security in the first place. Being stuck in the bad equilibrium has negative consequences for everyone involved.

Note that we do not claim that cloud computing does not create business today. The industry is growing rapidly [30]. But the bottom line of the literature presented is clear: Trust concerns hinder cloud computing to develop its full technical, social, and economic potential. Any proposal that increases trust is therefore welcome. We contribute to such a proposal in this paper by distinguishing those institutions that can effectively increase trust in the cloud from those that cannot.

III. The Case for Private Ordering

Before applying the classification of contract enforcement institutions we question one important assumption that has been made in the literature, namely that "markets only work when governments provide a framework of trust." (quotation attributed to Daniel Weitzner, US Deputy Chief Technology Officer for Internet Policy, quoted by [14]). Rephrased, that claim says that private transactors depend on rules enforced by public institutions in order to work well.

We hold, in contrast, that it is unclear that regulation and contracts that rely on any kind of enforcement by public authorities in case of breach, are building blocks of an appropriate solution to the accountability problems in cloud computing. The main reason for this skepticism is up to the international, dynamic nature of the cloud computing industry identified as a major hurdle for its development [24]. The fact that the value chain that is involved in the production of cloud services is multinational creates a high demand for international legal and regulatory coordination in order to be effective – a level of coordination that has rarely been achieved in other industries. Without such coordination, however, CSPs who are either unwilling or unable to behave accountably will have few difficulties to move their nominal or de facto operations or file servers to jurisdictions with less stringent rules or less stringent enforcement of rules. This is likely to create a race to the bottom among governments around the world, eroding legal and regulatory restrictions on CSPs more and more. Such a development would be detrimental to the trust of consumers in cloud services.

Moreover, the dynamic nature of cloud computing, including unforeseeable technological innovations in the years to come, places a high value on a flexible and easy-to-adjust set of rules governing the behavior of industry participants. Democratic parliaments formulating laws, public agencies setting up regulatory rules, and public courts enforcing contracts are not characterized by the flexibility and case by case interpretation of rules that dynamic industries require.

Therefore, we argue that the optimal governance institution for the cloud computing industry is characterized by *private ordering* or self-governance, that is, a set of behavioral and enforcement rules that are fully administered by private parties, where any breach of rules is punished in a clearly specified way by pre-determined other private parties, and where each party involved has no incentive to change its purported behavior as long as the other parties do not change their behavior [33]. Below we will outline some key characteristics of such a private ordering solution.

IV. Narrowing Down the Set of Feasible Institutions

We rely on Greif's definition of institutions, which consists of two parts [15]. First, an institution is a set of rules regarding behavior in a *central transaction,* which is the transaction that can create value for the participants but where both good and bad behavior is possible. Good behavior in the central transaction is supported by an *auxiliary transaction*, which consists of a punishment rule and an allocation of the responsibilities who is to punish a party that behaved badly in

the central transaction. In cloud computing the central transaction refers to CSPs' fulfilment or non-fulfilment of their contractual obligations towards their customers to implement a high level of security and accountability. The auxiliary transaction depends on the enforcement institution used.

Masten and Prüfer [19] propose a classification of contract enforcement institutions; see Figure 1. This scheme lists and classifies potentially available enforcement institutions in general. The application to cloud computing follows below.

The classification refers to situations where two individuals could engage in jointly beneficial trade with each other ("cooperate") but at least one party has an incentive to shirk and to maximize her own payoff at the expense of her partner ("defect"); a so-called Prisoner's Dilemma. Referring to Greif's terminology, the Prisoner's Dilemma occurs in the central transaction. Each institution in Figure 1 can be at the heart of an auxiliary transaction that punishes defectors in one way or the other.

Many buyer-seller relationships in the cloud computing industry are characterized by "one-sided" Prisoner's Dilemmas: the buyer of a service, who can either be an individual user or a firm outsourcing some data processing or storage to another CSP, values a high level of accountability. Therefore, she would be willing to pay a high price for such a service. For the seller, in contrast, providing a high level of accountability is costly. Hence, *ceteris paribus* she would prefer to save some cost by providing less accountability. Assume that the service agreement or contract between the seller and the buyer includes an obligation of the seller to provide a high accountability level (otherwise, there is no economic problem to be solved). Then, if the buyer understands the incentive of the seller to produce little accountability, the buyer will only be willing to pay a low price for the service. But given this low willingness-to-pay of buyers, only sellers who actually supply low accountability will populate the market. This is the classical adverse selection or lemons problem in economics [2]. It applies to all types of cloud computing services, be it Cloud Software as a Service, Cloud Platform as a Service, or Cloud Infrastructure as a Service [21]. See [3] and [8] for more detailed discussions.

Masten and Prüfer's classification categorizes the governance institutions that can potentially solve the transactors' problem. *Internal value system* refers to situations where the seller would not renege on her contractual obligations because she is is ethically motivated to act as promised. Such ethics can install cooperative behavior, by definition, but the problem is that it is very hard to affect the preferences of industry participants regarding the wellbeing of their trade partners, to which they are not bound by close ties [7], [11]. Hence, internal value systems cannot solve the trust issues involved in cloud computing by a significant scale.

The next enforcement institution, labeled *Bilateral Interaction* refers to situations where the same two players interact with each other repeatedly and, hence, can threaten to cease the relationship with each other in case of defection [18].

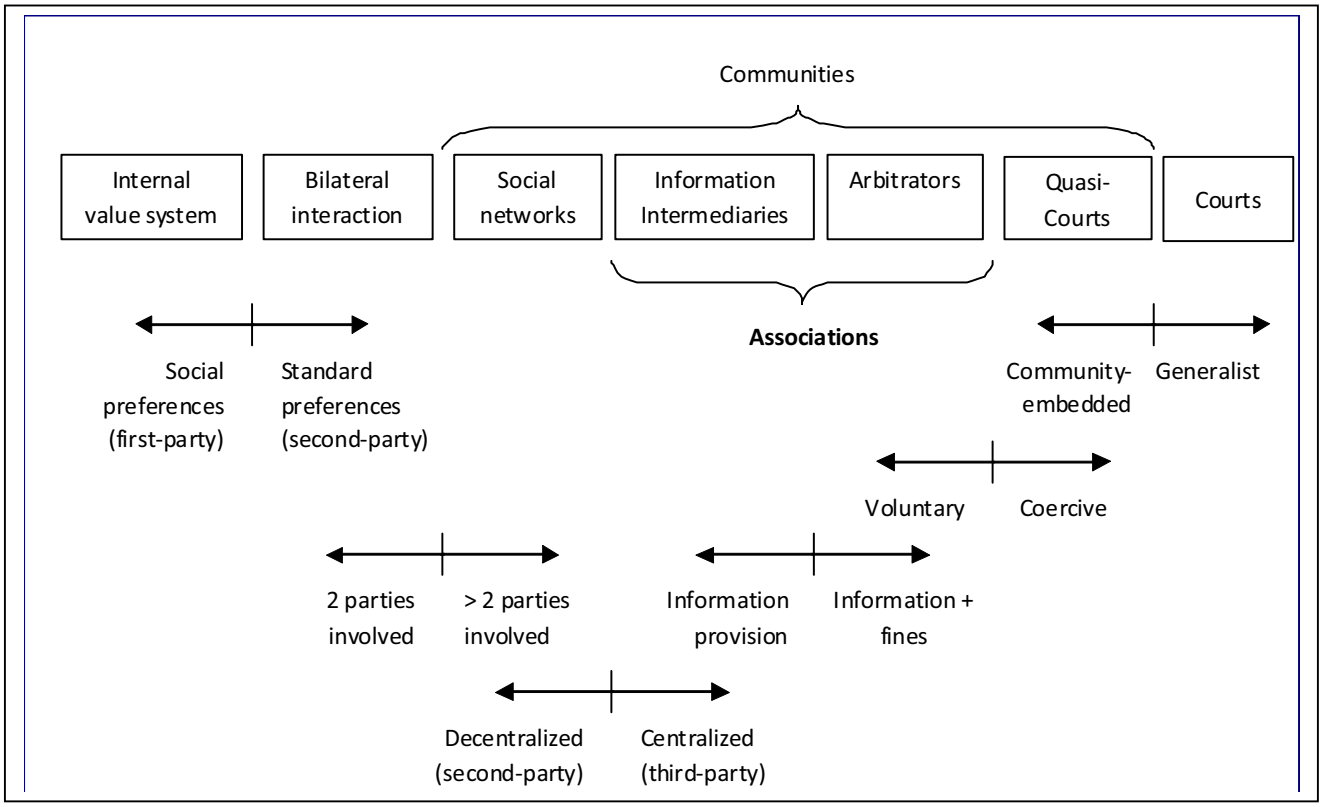

Fig. 1. A Classification of Contract Enforcement Institutions. Adapted from [19].

Cloud computing, as other dynamic industries with many players involved, is not characterized by such stable bilateral relationships. Hence, this institution also offers no solution.

In *Social Networks* the threat to cease a long-term relationship is extended to the friends or other close (business) partners of the interacting transactors. If service provider A defects in a relationship with user B, B will inform his friends, users C and D, about the defection. If A tries to sell her services to C or D in the future, they may not trade with her because they know that A defected in the past. Hence, by cheating B, A risks losing business in the future. If A understands this threat, A's propensity to defect is mitigated.

Notably, however, social networks as an enforcement institution rely on the decentralized transmission of information about the business conduct of each and every CSP and on the incentives to also punish defectors in a decentralized fashion by ostracising them from the community of (honest) traders. If information about individual players' behavior is hard to communicate or if network members can easily receive contradicting messages about someone's behavior, social networks work imperfectly. This is especially true if the best connected players are the largest and, therefore, most profitable ones to do business with in the future for others because these powerful members have strong incentives to defect themselves. Smaller network members learning about such a defection may be in conflict whether it is worth refusing to trade with the big player or whether a refusal would hurt themselves even more.

Therefore, social networks as an enforcement mechanism are particularly powerful if the traders are well connected to other traders, if the importance of traders is rather symmetric, and if the total number of traders is limited. This point has been made by theoretical and empirical studies [9], [15], [22]. It can be shown by means of a game-theoretic model that the effectiveness of social networks diminishes the larger the value of a single transaction is for the partners or the lower the average connectedness of the network members is [19]. Given that we want to encourage users to put their most precious data to the cloud, this constraint is hurt.

Moving to the very right of the figure, public *Courts* can enforce contracts by using coercion. Due to the high damage coercion can do to transgressors, the threat of coercion can deter many defections. The problem is, however, that general courts are bound by strict rules, which make them relatively slow, inflexible, and expensive to use, as compared to private enforcement mechanisms. Therefore, courts might not be used in equilibrium for low to medium valued transactions [19]. The sheer presence of courts may even crowd out private enforcement mechanisms and thereby destroy existing ostracism-based institutions [19]. As argued above, this problem is amplified by the international and dynamic nature of the cloud computing industry, where often many parties (data controllers and data processors) are involved in the production of one service sold to individual or business users.

Note that the problems posed by the international nature of the cloud computing industry could be mitigated by recent EU and US regulation that de facto extends the power of national or EU public enforcement agencies (courts and regulators) to CSPs producing cloud services outside of their traditional jurisdictional boundaries. Such extraterritorial extensions of juridictional powers are highly problematic from a legal perspective, though, and come at unpredictable costs, e.g. for trade wars between the jurisdictions involved or a cyber arms race between those states who extend their jurisdictions and those who insist on their sovereignity [28], [30].

The other institution in the figure with access to coercion is termed *Quasi-Courts*. It comes in two shapes: as *specialized public courts* (e.g. commercial courts) who operate with more flexible decision making rules than general courts and are often staffed by experts in the subject (e.g. business people), not jurists; and as *criminal organizations* (e.g. the mafia) who illegally reserve the right to enforce their decisions with coercion. Both shapes combine coercive enforcement with community embeddedness: their decision making procedures are less strict and rule-based than general courts'. Instead, quasi-court judges have more discretion and can use soft information about the business conduct of litigants.

Although this combination of coercive powers and community embeddedness may seem attractive, quasi-courts also have distinct downsides [20]. Regarding cloud computing, on the one hand specialized courts backed by access to public enforcement suffer from the same problems – international and dynamic nature of the industry – than general courts; see section III. On the other hand, due to their non-democratic, exclusive decision making rules and profit-maximization, criminal organizations are also no role model for the optimal enforcement institution in cloud computing, which is discussed in more detail in [8] and [13].

This leaves *Associations* as organizations around which an appropriate institution is built. Business or trade associations are private, formal, noncommercial organizations designed to promote the common business interests of their members [27]. They have their own legal entity and, regarding contract enforcement, assist their members in disputes that can either involve two members or one member and one non-member. To finance their operations, associations charge a membership fee. In some cases associations can rely on state enforcement but their main enforcement tool is ostracism. Given the general problems of public enforcement in cloud computing discussed above, we focus on private enforcement here. If the association has information about defective business conduct of a player in the industry and that behavior is not recouped appropriately, the wrongdoer will be blacklisted and lose future business with all association members [26], [32].

In practice, associations have several tasks. For contract enforcement purposes, two of them are particularly important, as displayed in the figure: *Information Intermediaries* (such as credit bureaus), who collect information about the business conduct of many industry participants and disseminate that information among their members; and *Arbitrators*, who investigate a case upon a member's request and determine damage payments from the defector to the victim in case they find any contract infringement. Notably, damage payments have to be self-enforcing, that is, they will only be paid if the damage payment is less than the net present value of doing business with association members in the future.

One of the main advantages of arbitration tribunals over public general courts is that the latter operate under rigid procedural rules, whereas arbitration tribunals can use procedures that are self-determined by – and therefore customized to the needs of – their members. This reduces procedural costs and makes arbitration tribunals more effective. For instance, whereas the burden of proof is a clearly defined threshold plaintiffs in front of general courts have to produce, arbitration tribunals can reduce the burden of proof if the characteristics of the transaction make the change reasonable.

V. The Optimal Governance Institution: a Certification Agency

In cloud computing, an information intermediary could be an entity that collects all information available on the relevant conduct of every CSP - e.g. about how it treats security leaks, what the quality of service is, etc. – and publicizes this information to all interested parties. This body could be a *certification agency* that provides CSPs with a certificate for "accountable cloud services" if they meet quality standards that are regularly monitored by the agency [4]. It should be a privately set up and managed nonprofit organization, where "membership" (seeking certification) is a choice variable for CSPs (cf. the problems of public enforcers discussed above).

A key advantage of such a certification agency over informal governance institutions is that it can efficiently reduce complexity. In practice, accountability is a multidimensional problem that encompasses technical, organizational, legal, and other dimensions in which a trustworthy CSP must perform. A certification agency could define minimum levels of required performance in each of these dimensions and only award certificates to CSPs who fulfil the minimum levels in all dimensions. Therefore, the complex multidimensional problem requiring detailed technical expertise, which would have to be solved by every user individually in the absence of certification agencies, is reduced to a one-dimensional Bernoulli distribution: users can base their consumption choices upon the information whether a CSP is certified, or not.

In order to be credible, the certification process would have to include extensive, ongoing tests, at random intervals to ensure the results validity; see [25] for more details regarding the technical requirements. But such testing is costly, and we suggest to make CSPs pay for their own certification process, as is done in other certification areas such as environmentally and socially beneficial forest management [https://ic.fsc.org/index.htm].

Why would a cloud service provider apply (and pay) for the services of a certification agency? The answer is that, if consumers only buy services from certified providers, being certified (and fulfilling certification standards) becomes a business necessity for CSPs. Why would consumers only buy from certified CSPs, in particular if these could be more expensive than uncertified CSPs? Depending on consumer preferences, there may arise a differentiated market in equilibrium: an "accountable" segment with certified, accountable CSPs charging relatively high prices who sell to business consumers with high security demands and to individual consumers with a high preference for privacy; and a "nonaccountable" segment with uncertified CSPs selling services of uncertain security (from consumers' perspective) for lower prices. Most likely, the type of data hosted by the latter segment would be less crucial for businesses or the respective consumers would be less concerned about privacy.

If such an organization only publicizes information that is self-reported by CSPs, it would be classified as an information intermediary in the figure above. If it would actually check information for correctness with own employees and own software systems itself and, in particular, if it would actively punish CSPs who report false information or who do not act accountable, by withdrawing a certificate or even award damage payments from wrongdoers to their victims, it would be classified as an arbitrator.

"[O]nly if the arbitrator is sufficiently competent to decide a case correctly, an arbitration association can outperform an information association with respect to supporting cooperative trade" [26: p.24]. Another important condition is that the costs to operate a tribunal are not excessive. On the upside, because arbitration tribunals qualify the information of plaintiffs about their business partners' conduct by investigating cases themselves, the risk of ostracising a trader on false grounds is lower with arbitration tribunals than with information intermediaries. The stakes in cloud computing, measured by the total turnover of the industry, are high and growing. Therefore, we perceive *certification agencies with arbitration tribunals* as the best institution available to mitigate economic governance problems in the cloud computing industry.

VI. Conclusion

Starting from the threat of insufficient market development of cloud computing technologies, in this paper we have analyzed which governance institution may be best suited to solve the problems stemming from asymmetric information about the true level of data protection, security, and accountability offered by cloud service providers. We concluded that, due to the characteristics of today's cloud computing industry, the optimal institution be characterized by private ordering, not public ordering. Moreover, the institution's mechanism to ruin defectors' reputation as a trustworthy transactor has to be quick, easy to understand, and the information about CSPs' accountability levels needs to reach many consumers quickly and credibly. We have found that certification agencies are institutions matching these requirements closest: privately managed nonprofit organizations with an own legal entity that are staffed by industry experts and rely on contract enforcement via ostracism, not public coercion (i.e. ruining defectors' reputation by withdrawing a certificate as soon as the accountability threshold required for certification is hurt).

Such a certification agency can monitor the accountability levels of CSPs as far as technically possible and provide providers of high accountability with a certification label that can easily be detected by private and business users. Users with high valuation for accountability will be willing to pay more for the services of certified CSPs – which makes the investments in accountability worthwhile for some CSPs - whereas other users may purchase from uncertified CSPs

saving on those investments [5]. One precondition for a successful agency may be to include representatives of both CSPs and users, on the board of the certification agency in order to give a voice to all concerns and have a platform to discuss and to mediate conflicts between these groups. This board should define the accountability requirements to get certification and to make sure that the institution is well known on both sides of the market.

These theoretical predictions could be best tested empirically by introducing a certification agency for a limited set of cloud services and to study whether the predicted vertical differentiation of cloud services occurs in practice, or not. As a pre-test, it may be possible to use a trust certificate in a related Internet market, which follows the certification structure outlined here, and test how randomly displaying or not displaying the certificate of a CSP's website affects its sales.

The most pressing issue that follow-up research is to take up is the solution of the certification agency's *credibility problem*: the governance structure of the agency has to make sure that it cannot be corrupted itself and that its employees do not have any incentive to misreport the findings of their monitoring task [10]. Setting up the agency as a nonprofit organization, to take away the incentive to get captured by CSPs who pay the agency for certificates, is a first but insufficient step. One potential solution is to invoke competition among certification agencies in order to reduce the potential of one agency abusing a powerful market position. If several certification agencies exist, however, standardization among their certification protocols is important [4].

ACKNOWLEDGEMENTS

We are grateful to seminar participants at TILEC and at A4Cloud, especially to Eleni Kosta and Maartje Niezen, who provided valuable feedback on an earlier draft of this paper. We also thank Massimo Felici and three anonymous referees for their constructive input. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4Cloud).

REFERENCES

[1] Acquisti, Alessandro. 2010. "The Economics of Personal Data and the Economics of Privacy," OECD Roundtable Contribution.

[2] Akerlof, George. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," Quarterly Journal of Economics, 84 (3): 488-500.

[3] Axelrod, Robert. 1984. The Evolution of Cooperation. Basic Books.

[4] Backhouse, James, Hsu, Carol, Tseng, Jimmy and John Baptista. 2005. "A Question of Trust," Communications of the ACM, 48(9): 87-91.

[5] Baye, Michael and John Morgan. 2003. "Red queen pricing effects in e-retail markets," SSRN working paper 655448.

[6] Catteddu, Daniele and Giles Hogben. 2009. "An SME perspective on Cloud Computing," ENISA survey.

[7] De Dreu, Carsten K. W., Greer, Lindred L., Handgraaf, Michel J. J., Shalvi, Shaul, Van Kleef, Gerben A., Baas, Matthijs, Ten Velden, Femke S., Van Dijk, Eric and Sander W. W. Feith. 2010. "The Neuropeptide Oxytocin Regulates Parochial Altruism in Intergroup Conflict Among Humans," Science, 328: 1408-1411.

[8] Dixit, Avinash. 2003a. "On Modes of Economic Governance," Econometrica, 71: 449-81.

[9] Dixit, Avinash. 2003b. "Trade Expansion and Contract Enforcement," Journal of Political Economy, 111(6): 1293-1317.

[10] Edelman, Benjamin. 2011. "Adverse selection in online 'trust' certifications and search results," Electronic Commerce Research and Applications, 10, 17–25.

[11] Ermisch, John and Diego Gambetta. 2010. "Do strong family ties inhibit trust?" Journal of Economic Behavior & Organization, 75: 365-376.

[12] Etro, Federico. 2009. "The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe," Review of Business and Economics, 54(2): 179-208.

[13] Gambetta, Diego. 1996. The Sicilian Mafia: The Business of Private Protection. Harvard University Press.

[14] Godel, Moritz, Litchfield, Annabel and Iris Mantovani. 2012. "The Value of Personal Information Evidence from Empirical Economic Studies," in: Bonneau, Vincent et al., "Dossier on Privacy, Openness and Trust," Communications & Strategies, 88 (4), 41-60.

[15] Greif, Avner. 2006. Institutions and the Path to the Modern Economy: Lessons from Medieval Trade. New York: Cambridge University Press.

[16] Haeberlen, Andreas. 2010. "A Case for the Accountable Cloud," ACM SIGOPS Operating Systems Review, 44(2), 52-57.

[17] Jentzsch, Nicola, Preibusch, Sören and Andreas Harasser. 2012. "Study on Monetising Privacy. An Economic Model for Pricing Personal Information," ENISA report.

[18] MacLeod, W. Bentley. 2007. "Reputations, Relationships, and Contract Enforcement," Journal of Economic Literature, XLV (September): 595-628.

[19] Masten, Scott E. and Jens Prüfer. 2011. "On the Evolution of Collective Enforcement Institutions: Communities and Courts," CentER Discussion Paper, No. 2011-74.

[20] Masten, Scott E. and Jens Prüfer. 2013. "General and Specialized Courts: Objectivity vs. Expertise in Adjudication," mimeo.

[21] Mell, Peter and Tim Grance. 2009. "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory.

[22] Ostrom, Elinor. 1990. Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge, UK: Cambridge University Press.

[23] Pearson, Siani, Catteddu, D., Felici, M., Hogben, G., Papanikolaou, N., and D. Pradelles. 2012. "Scoping report and initial glossary", A4Cloud project report, version 0.71.

[24] Pearson, Siani. 2011. "Toward Accountability in the Cloud", IEEE Internet Computing, 15(4), 64-69.

[25] Probst, ChristianW., Sasse, M. Angela, Pieters, Wolter, Dimkov, Trajce, Luysterborg, Erik and Michel Arnaud. 2012. "Privacy Penetration Testing: How to Establish Trust in Your Cloud Provider," European Data Protection: In Good Health?, 251-265.

[26] Prüfer, Jens. 2012. "Business Associations and Private Ordering," CentER Discussion Paper, No. 2012-094.

[27] Pyle, William. 2005. "Contractual Disputes and the Channels for Interfirm Communication," Journal of Law, Economics, and Organization, 21(2): 547-575.

[28] Soghoian, Christopher. 2010. "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era," Journal on Telecommunications and High Technology Law, 8(2).

[29] The Economist. 2013a. "The IT cloud: Silver linings," July 20, 2013.

[30] The Economist. 2013b. "Reaching for the clouds," July 20, 2013.

[31] The Guardian. 2013. "Why NSA surveillance is a threat to British doctors and lawyers," June 20, 2013.

[32] Wall Street Journal. 2012. "Cotton-Contract Crackdown," September 3, 2012.

[33] Williamson, Oliver E. 2002. "The Lens of Contract: Private Ordering," American Economic Review P&P, 92(2): 438-443.