Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution

By: Nir Kshetri

Kshetri, Nir (May–June 2013). "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution," *Telecommunications Policy*, 37(4–5): pp. 372–386.

Abstract:

Cloud computing is likened and equated to the Industrial Revolution. Its transformational nature is, however, associated with significant security and privacy risks. This paper investigates how the contexts provided by formal and informal institutions affect the perceptions of privacy and security issues in the cloud. This paper highlights the nature, origin, and implications of institutions and institutional changes in the context of cloud computing. A goal of the present work is also to gain insights into the mechanisms and forces that have brought about institutional changes in the cloud industry. Specifically, they investigate how contradictions generated at various levels by the technology, the formation of dense networks and relationships and the changing power dynamics have triggered institutional changes. Since the current analysis of the causes and consequences of institutions and institutional change is mainly concerned with more established industries and markets, this paper is expected to provide insights into institutions surrounding to this new and emerging technological development.

Keywords: privacy | security | cloud computing | institutions | institutional changes | trust production process | contradictions | telecommunications

Article:

1. Introduction

Cloud computing (hereinafter: cloud) is described in the popular press as the next big thing and a major technology disruption (Weber, 2011). It is likened and equated to the Industrial Revolution in terms of implications for technological innovations and economic growth (Price, 2011). At the same time, the transformational nature of the cloud is associated with significant security and privacy risks.

A significant gap remains between vendors' claims and users' views of the cloud's security, privacy and transparency. The cloud industry's response has been: Clouds are more secure than whatever you're using now (Talbot, 2010). But many users do not agree. Issues such as security, privacy and availability are among the topmost concerns in organizations' cloud adoption decisions rather than the total cost of ownership (Brodkin, 2010 and McCreary, 2008; Table 1). Allen (2011, p. 3) notes: “One of the largest disadvantages of cloud computing revolves around security and confidentiality”. Due primarily to concerns related to security, privacy and confidentiality critics have argued that its perceived costs may outweigh the benefits (Tillery, 2010). Organizations worry about hidden costs associated with security breaches or lawsuits tied to data breach. Businesses and consumers are cautious in using it to store high-value or sensitive data and information (Goodburn & Hill, 2011).

Table 1.

Organizations' perceptions of the cloud's security: Some representative surveys.

Survey conducted by	**Conducted/released in**	**Major findings**
IDC	October 2008	• Security concern was the most serious barrier to cloud adoption for organizations.
Information week	2009 and 2010	• 31% of companies in 2010 viewed SaaS Apps as less secure than the internal systems compared to 35% in 2009 (Ely, 2011).
IDC (conducted in Asia-Pacific)	April 2010	• Less than 10% of respondents were confident about cloud security measures.
Harris Interactive survey for Novell	October 2010	• 90% were concerned about cloud security. • 50 viewed security concerns as the primary barrier to cloud adoption. • 76% thought private data more secure when stored on the premises. • 81% were worried about regulatory compliance.

Survey conducted by	Conducted/released in	Major findings
IDC	2011	• A third of IT executives feel the benefits of cloud exceed risks. • About a quarter did not fully understand the regulatory and compliance issues in cloud computing, *a*. • 47% concerned about a security threat (Ricadela, 2011)
Cisco's CloudWatch 2011 report for the U.K. (research conducted by Loudhouse)	September 2011	• 76% of respondents cited security and privacy a top barrier to cloud adoption. • 64% of respondents concerned about location of data (Nguyen, 2011).

The central argument of this paper is that security and privacy issues in the cloud, which are real as well as perceived phenomena, can be better understood by examining the formal and informal institutions. Due to the lack of development in cloud-related legal systems and enforcement mechanisms, privacy, security and ownership issues in the cloud fall into legally gray areas (Bradley, 2010). Some argue that if an organization dealing with customer data stores them in the cloud provided by a vendor, the organization rather than the vendor is likely to be legally responsible if customer data are compromised (Zielinski, 2009). This is because while the organization may face a lawsuit from the victims, the vendor may not have to take responsibility under the existing institutional arrangements. Some commentators have argued that there has been arguably a “disturbing lack of respect for essential privacy” among cloud providers (Larkin, 2010, p. 44). For instance, in a complaint filed with the Federal Trade Commission (FTC), the Electronic Privacy Information Center (EPIC) argued that Google misrepresented privacy and security of its users' data stored in the Google cloud (Wittow & Buller, 2010). Cloud providers are also criticized on the ground that they do not conduct adequate background security investigations of their employees (Wilshusen, 2010).

The issues related to security and privacy in the cloud, while well documented, are only partially understood. A clearer understanding of various institutional actors, their actions and how they are shifting would help organizations navigate the complex, turbulent and rapidly evolving cloud landscape. Researchers have paid relatively less attention to how the structure of the markets, legal and political environment as well as inter-organizational and intra-organizational

arrangements affect the ways in which investment decisions are made. This paper seeks to fill part of this void by examining the role of institutions and institutional evolution concerning cloud security and privacy.

Before proceeding, some clarifying definitions are offered. Institutions are the “rules of the game” (North, 1990, p. 27) and include “formal constraints (rules, laws, constitutions), informal constraints (norms of behavior, conventions, and self-imposed codes of conduct), and their enforcement characteristics” (North, 1996, p. 344). Cloud computing involves hosting applications on servers and delivering software and services via the Internet. In the cloud computing model, companies can access computing power and resources on the cloud and pay for services based on the usage. Cloud industry is defined as the set of sellers/providers of cloud related products and services.

Cloud providers or vendors, which are suppliers of cloud services, deliver value to users through various offerings such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). SaaS is a software distribution model, in which applications are hosted by a vendor and made available to customers over a network. It is considered to be the most mature type of cloud computing. In PaaS, applications are developed and executed through platforms provided by cloud vendors. This model allows a quick and cost-effective development and deployment of applications. Some well-known PaaS vendors include Google (Google App Engine), Salesforce.com (Force.com), and Microsoft (Windows Azure platform). Some facilities provided under PaaS model include database management, security, workflow management, and application serving. In IaaS, compute power and storage space are offered on demand. IaaS can provide server, operating system, disk storage and database, among other things. Amazon.com is the biggest IaaS provider. Its Elastic Compute Cloud (EC2) allows subscribers to run cloud application programs. IBM, Vmware and HP also offer IaaS.

The remainder of the paper proceeds by first presenting the theoretical framework. Next, institutions and institutional evolution in the cloud industry are discussed. Then, the forces and nature of institutional changes in the cloud industry are examined. It is followed by a section on discussion and implications. The final section provides concluding comments.

2. The theoretical framework: Institutions and institutional changes

The cloud industry is undergoing a major technological upheaval. In most cases, such changes create confusion and uncertainty and produce an environment that lacks norms, templates, and

models about appropriate strategies, structures and sources of legitimacy (Newman, 2000). Existing institutions are inadequate and obsolete to deal with the security and privacy problems facing the cloud. For instance, the cloud has challenged traditional institutional arrangements and notions about auditing and security (Messmer, 2010).

Formal and informal institutions affect perception of legitimacy and trustworthiness of the cloud. The responses to technological innovations of institutional actors such as technology developers, users and regulators, however, tend to lag behind the innovations (Katyal, 2001). Moreover, institutional actors vary in their timing of responses due to different vested interests, capability to respond and various levels of understanding about the issues. In addition, research conducted in other industry sectors indicates that organizations may have different approaches to ethical decision making in their interactions with other businesses, consumers and the government (Whitcomb, Erdener, & Li, 1998). While trade and professional associations and industry bodies have responded to security and privacy issues, government agencies have been slow to adopt necessary legislative and regulatory measures to monitor users and providers.

Institutional theory deals with the issue of seeking legitimacy, approval and support from various actors in the environment (Dickson et al., 2004 and Campbell, 2004). Institutional influence in the cloud industry becomes an admittedly complex process when cloud providers and their clients need to derive legitimacy from multiple sources such as employees, clients, client's customers, professional/trade associations and governments.

Scott (2001) proposed three institutional pillars: (i) regulative; (ii) normative and (iii) cognitive. These pillars relate to “legally sanctioned”, “morally governed” and “recognizable, taken-for-granted” behaviors, respectively (Scott, Ruef, Mendel, & Caronna, 2000, p. 238). The following examples illustrate the three pillars from the standpoint of cloud security and privacy.

The European Union (EU) countries' strong data privacy laws prevent the movement of identifiable individuals' data to jurisdictions that do not provide the same levels of protection. These regulative institutions have arguably hindered the diffusion of the cloud in the EU countries (Bradner, 2010).

Many cloud vendors emphasize their security credentials by communicating to clients that they have completed the Statement on Auditing Standards (SAS 70) audit (Brodkin, 2010). Note that

the SAS 70 Audit developed by the American Institute of Certified Public Accountants (AICPA) represents that a service organization has been “through an in-depth audit of their control objectives and control activities” which may include controls over IT and related processes (SAS 70 Overview, 2011). By communicating about their SAS 70 compliance, they are emphasizing on normative institutions related to the cloud industry. An organization's cloud adoption decision may also depend on its perception of the providers' ability to protect data from a third party, make them available when needed and a trust that the provider would not engage in opportunistic behavior. This mental map can be described as a component of cognitive institutions (Talbot, 2010).

2.1. Institutional field

Drawing on the analysis of Schumpeter (1939), Antonelli (1993, p. 621) points out that an analysis of “the collective character of the innovation process, the interdependence among innovators, and the complementarity of the new technologies within the gales of innovations”, and the “intertwined co-evolution of economic institutions, industrial structures, economic architectures of interactions and exchanges and consumers' preferences along with the innovative process” would offer important insights into the “systemic and inherently complex character of the innovation dynamics”. To put things in context, security and privacy issues are shaped by expectations, values, positions, power, influence, resources, roles, concerns, orientation and interests of various institutional actors that have different levels of understanding and are affected differentially by these issues. In this regard, the idea of institutional field can be helpful in understanding institutions and institutional changes associated with the cloud.

An institutional field is “formed around the issues that become important to the interests and objectives of specific collectives of organizations” (Hoffman, 1999, p. 352). For the cloud industry, this institutional field includes national governments, supra-national organizations, industry bodies, trade and professional associations as well as cloud vendors, cloud clients and the organizations of these clients (Fig. 1, Table 2). The “content, rhetoric, and dialog” among these constituents influence the nature of field formed around the cloud (Hoffman, 1999, p. 355).

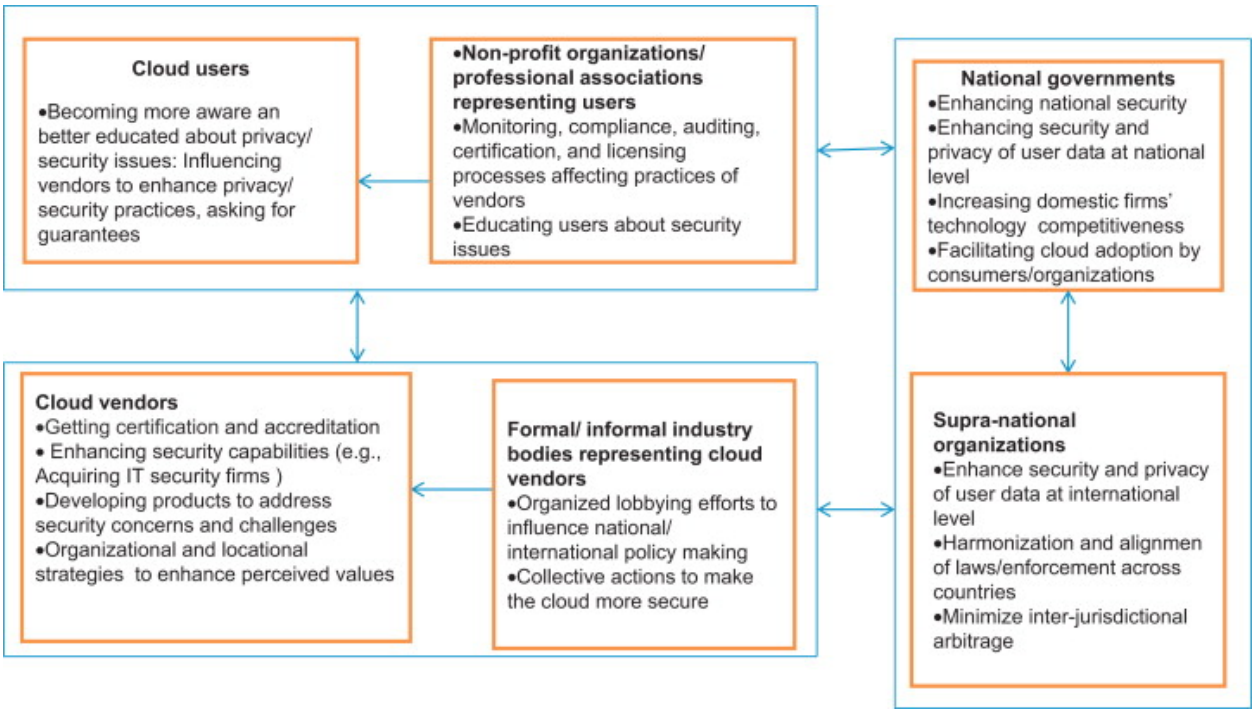

Fig. 1.

Actions of and interactions among various institutional actors associated with the cloud industry.

Table 2.

A sample of actions and responses of various actors in shaping cloud related institutions.

Actor	Nature and sources of powers	A sample of actions
Cloud users	Relative power vis-a-vis the providers has increased with an intense competition.	• After users' complaints about data ownership issues, Dropbox updated its user terms/conditions.
Cloud vendor	Decreasing relative power but attempting to increase potential power by offering users with new, innovative and potentially attractive value propositions.	• HiDrive Free: conform to the ISO27001 security standard. • Epsilon and AWS: SAS 70 certified. • Salesforce.com's acquisition of Navajo Systems for $30 million (Team, 2011). • Dell's acquisition of SecureWorks (Claburn, 2011). • To win federal-government deals, AWS and Google undertook efforts to improve security to achieve certification for FISMA. • HiDrive Free: hosted at German data centers, which ensures that its service conforms to German privacy

Actor	Nature and sources of powers	A sample of actions
		laws, which are among the world's strictest (Cooter, 2011).
Associations representing cloud users	Norms, informal rules, ethical codes and expert power.	• AICPA's official endorsements to Paychex, Intacct and Copanion. • CSA: as an independent voice promotes the use of best practices for providing security assurance and provides education for users.
Inter-organizational bodies representing cloud vendors	The power of collective action.	• ETNO: lobbied for an international privacy standard, simplification of rules governing data transfers, and others—expected to enable European companies to compete with those in the U.S. (Ingthorsson, 2011). • Oracle, Cisco Systems, SAP, Apple, Google and Microsoft: lobbied to streamline EU's fragmented national data protection laws. In January 2011, Microsoft general counsel, spoke to the French National Assembly to lower cloud barriers (O'Brien, 2011). • The OASIS IDCloud TC: works to address security challenges associated with identity management and develops guidelines for overcoming vulnerabilities.
National governments	Coercive power over citizens and businesses.	• FISMA in the U.S.: cloud providers are required to keep sensitive data belonging to a federal agency within the country. • The U.S. and the U.K.: legislations governing the location of storage for personal and medical data. • China's investment of US$154 million to develop a cloud center for high-tech and start-up firms in Chongqing. The cloud computing Special Administrative Region (SAR) will be free of the country's strict internet censorship filters (Russell, 2011). • European countries considering relaxing strict data privacy laws to facilitate cloud adoption (European Commission 2010).
Supra-national institutions	Nations mostly observe principles of international law and obligations: can resolve transnational problems.	• EU planning to make mandatory to notify customers of data breaches. • European Parliament's Civil Liberties Committee: recommended making easier for users to access, amend and delete data and appointing dedicated data protection officers in companies (Worth, 2011).

Actor	Nature and sources of powers	A sample of actions
		• European Commission: emphasizing the importance of easing users to change cloud provider by developing de facto standard for moving data among different clouds (overcoming the lock-in). • EU members working to align privacy laws and close jurisdictional gaps.

Institutional theorists make an intriguing argument as to how a field evolves. A field is a dynamic system characterized by the entry and exit of various players and constituencies with competing interests and disparate purposes and a change in interaction patterns among them (Barnett & Carroll, 1993). As is the case of any issue-based field, these players continuously negotiate over issue interpretation and engage in institutional war (Greenwood & Hinings, 1996). This dynamics in the context of the cloud industry is presented in Fig. 1. The last column of Table 2 provides a sample of actions related to the boxes in Fig. 1.

Prior researchers have noted that fields evolve through three stages (Purdy & Gray, 2009). In the innovation stage, new logics related to security and privacy concerns in the cloud are introduced and are drawn into debate. The cloud industry is probably in the second stage, mobilization, in which field development is characterized by a complex power dynamics. For instance, cloud providers are attempting to exercise their power based on expertise, experience and knowledge and are engaging in technology push without sufficiently addressing the security and privacy concerns. Many users, on the other hand, are exercising their bargaining power and voicing frustration with vendors' failures to address these issues. At the same time, some governments are using the coercive power of the state to use the cloud in spying on citizens. Institutional actors such as cloud vendors, organizations using the cloud and regulators in this mobilization stage compete to validate and implement their logics. For instance, cloud vendors are relying on the economic logic of the cloud's low TCO to persuade cloud user. Some cloud users' logics are based on the idea that the cloud's costs are likely to outweigh the benefits in the absence of strong security measures. The final stage is the structuration stage, in which logics are translated into practices (Reay, Golden-Biddle, & GermAnn, 2006). In this stage, norms and structures are standardized and institutions deepen their taken-for-grantedness (Covaleski & Dirsmith, 1988). It is clear that institutional fields around the cloud have not yet reached the structuration stage.

Prior research indicates that institutional evolution entails transitions among the three institutional pillars—regulative, normative, and cultural-cognitive. Building a regulative/law pillar system is the first stage of field formation. It is followed by a formation of normative

institutions (e.g., assessment from ethical viewpoint) and then cognitive institutions (e.g., culturally supported belief) (Hoffman, 1999).

The formation of regulative pillar for the cloud industry would be characterized by the establishment of legal and regulatory infrastructures to deal with many issues including security and privacy. A normative institutional pillar is said to be established if ethical, and social views start influencing these issues. That is, rich and well developed ethical codes, guidelines and traditions develop in the cloud industry. Likewise, a cognitive pillar is established if cloud related decisions of organizations and individuals are culturally and cognitively determined.

3. Institutions and institutional evolution in the cloud industry

Another way to examine the factors related to privacy and security issues of the cloud is to consider a broad approach which defines the concept of institution in terms of a game's equilibrium. This framework is based on insights from game theory in which the basic idea is that agents (e.g., cloud vendors, users, etc.) would adopt strategies which are rational at the individual level. Three factors that determine an equilibrium include "(i) technologically determined external constraints; (ii) humanly devised external constraints, and; (iii) constraints developed within the game through patterns of behavior and the creation of expectations" (Snidal, 1996, p. 128). This section examines these factors, mainly (ii) and (iii), in the context of the cloud industry. Various institutional forces that are likely to push the cloud industry and markets towards equilibrium are presented in Table 2 and Table 3, and Fig. 1. Nature and sources of powers of various institutional actors associated with the cloud industry and some examples of their actions and responses in shaping cloud related institutions summarized in Table 2 and Fig. 1. Table 3 shows the possible institutional changes in the cloud industry as well as the associated mechanisms and forces.

Table 3.

Institutional evolution in the cloud industry.

Type of institutions	**Likely changes**	**Mechanisms/forces**
Regulative	Governments are likely to face pressures to strengthen cloud-related legal system and enforcement mechanisms.	• The transformational nature of the cloud forces the government to develop regulative institutions. • Spillover and externality effects may arise from the government agencies' demands of secure cloud for their use.
	Governments may face pressures to	• The globalization effect and position of international

Type of institutions	Likely changes	Mechanisms/forces
	harmonize and align their legal systems and enforcement mechanisms with those of other countries.	institutions to affect national policies.
Normative	Industry: processes for auditing cloud platforms are likely to evolve.	• Participants in an industry such as cloud computing benefit from compatibility and hence may push for a standard. • They are also interested in strengthening security and privacy issues.
	Professional and trade associations: are likely to emerge and influence security and privacy issues in new ways.	• In nascent and formative sectors such as cloud, there is no developed network of regulatory institutions. In such settings, professional and trade associations may emerge to play unique and important roles in shaping the industry. • They tend to have expertise, resources, experience and interests in this issue. • They may assess and monitor the performance of cloud vendors, which can help minimize risks for the members (e.g., AICPA).
Cognitive	Facing demanding consumers that are more aware and better educated about privacy/security, cloud vendors are likely to be equipped with improved mental map of the cloud environment.	• Cloud vendors are forced to engage in trust production processes. • Redistribution of power.
	Users may overcome the inertia effect.	• Users' expectations, values, and concerns about localness and control may change with thickening institutions and an understanding of and experience with the cloud.

3.1. Regulative institutions and their evolution

Regulative institutions consist of “explicit regulative processes: rule setting, monitoring, and sanctioning activities” (Scott, 1995, p. 35). In the context of this paper, regulative institutions consist of existing laws and rules, mainly enacted before the cloud era but are also relevant in the context of cloud computing. Some examples include the Sarbanes–Oxley (SOX) Act and the Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) in the U.S. To ensure the accuracy of financial data as required by the SOX compliance, IT controls need to be designed to ensure that data are accurate and are protected from unauthorized changes. HIPAA requires healthcare providers to have technical, physical and administrative security measures in place to protect the privacy, integrity, and availability of patients' data.

Those not complying with HIPAA standards may face up to $250,000 in fines and up to 10 years in prison.

3.1.1. Laws governing data in the cloud

The importance of regulative institutions such as laws, contracts and courts in the cloud industry should be obvious if this industry is viewed against the backdrop of the current state of security standards. The state uses coercive power in order to gain compliance. In the absence of radical improvements in security technology, such institutions become even more important because cloud users can rely on these institutions in case a cloud provider's failure to deliver a given level of security (Armbrust et al., 2010).

The cloud-related legal system and enforcement mechanisms are evolving more slowly compared to the technological development. Compliance frameworks such as the SOX and the HIPAA were developed for the non-cloud environment and thus do not clearly define the guidelines and requirements for data in the cloud (Bradley, 2010). Cloud computing thus poses various challenges for companies that have responsibilities to meet stringent compliance related to these frameworks such as IT disaster recovery and data security (NW, 2010).

The cloud also has several important new and unique features, which create challenges in writing contracts. For instance, a case concerning the contracts between Google and Computer Sciences Corporation (CSC) with the City of Los Angeles indicated several problems related to data breach and indemnification of damages. Google was a CSC subcontractor in the arrangement. An attorney analyzing the case noted that some of the complexity in the case would have been avoided if the term "lost data" was defined more clearly in the contracts (NW, 2010).

Some regulations governing the cloud are impractical and unclear. While it would not be practical to hold cloud providers liable for everything (TR, 2010), current regulations governing cloud security, which are derived from previous generations of technologies, arguably favor cloud providers. For instance, in the event of a data breach, the client, not the vendor, is likely to be legally responsible (Zielinski, 2009).

According to the Federal Information Security Management Act (FISMA), cloud providers are required to keep sensitive data belonging to a federal agency within the country. Google Apps used by government agencies are FISMA certified (Brodkin, 2010). Government agencies'

increasing use of the cloud and the fact that data security is extremely important for these agencies suggest that forward thinking governments may soon realize the need of clearer regulatory framework to address security issues. In addition, spillover and externality effects may arise from the government agencies' demands of secure clouds. A side effect of Google's delivery of secure clouds to government agencies is that private sector players are likely to become aware and interested in such services. Over time, Google thus may face pressure to provide the equivalent of FISMA certified Apps for the private sector as well.

3.1.2. International harmonization and alignment of legal system and enforcement mechanisms

Due to the globalization effect, governments are facing international pressures to harmonize and align legal systems and enforcement mechanisms. National governments are increasingly turning to supra-national institutions to resolve transnational problems (Smith & Wiest, 2005). Henkin (1979, p. 47) noted that “almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time”.

The cloud is also a matter of national competitiveness and security. Governments are thus enacting new laws and revising existing regulations to enhance the international competitiveness of domestic firms (Table 2, Fig. 1). In many cases, these actions have been in response to interest group pressures. For instance, industry associations such as the European Telecommunications Network Operator's Association (ETNO) as well as organizations such as Oracle, Cisco Systems, SAP, Apple, Google and Microsoft have been engaged in organized lobbying efforts to influence cloud related policies of the EU and its members (Fig. 1). The ETNO lobbied for an international online privacy standard and simplification of rules governing data transfers. It argued that these measures would enable European companies to compete on the same level as those in the U.S. (Ingthorsson, 2011). In response to these and other pressures, the EU and its members have shown willingness to enact cloud friendly laws, revise existing laws and collaborate with other institutional actors. The Vice-President of the European Commission responsible for the Digital Agenda, Neelie Kroes, for instance, emphasized the critical role the cloud can play in the economic growth of the member countries and emphasized the need to develop appropriate regulative framework (Thiel & Valpuesta, 2011).

3.2. Normative institutions and their evolution

Normative institutions introduce “a prescriptive, evaluative, and obligatory dimension into social life” (Scott, 1995, p. 37). This component focuses on the values and norms held by individuals and organizations that influence the functioning of the cloud industry. The basis of compliance in

the case of normative institutions derives from professional and social obligations. Non-adherence can thus result in societal and professional sanctions.

An association's norms, informal rules, and codes of behavior can create order, without the law's coercive power, by relying on a decentralized enforcement process where noncompliance is penalized with social and/or economic sanctions (North, 1990). A profession is self-regulated by codes of ethics, which require members to maintain higher standards of conduct than required by law (Backoff & Martin, 1991; Cohen & Pant, 1991).

Normative institutions also include trade/professional associations (e.g., the AICPA, and the European Telecommunications Network Operator's Association (ETNO)), industry groups or non-profit organizations (e.g., Electronic Privacy Information Center) that can use social/professional obligation requirements (e.g., ethical codes of conduct) to induce certain behaviors in the cloud industry and market.

A lesson from other economic sectors is that professional and trade associations are likely to emerge to play unique roles in shaping the industry in the absence of well-developed regulative institutions (Greenwood and Hinings, 1996 and Kshetri and Dholakia, 2009). There have already been some successful attempts at the association and inter-organizational levels to challenge the appropriateness of the current institutional arrangement. In the future even higher, broader and more significant institutional changes can be anticipated if only for the fact that the cloud has brought transformational shifts.

3.2.1. Associations representing cloud users

Professional associations are constantly emerging and influencing security and privacy issues in the cloud in new ways as a result of their expertise and interests in this issue. A visible example is the Cloud Security Alliance (CSA) (www.cloudsecurityalliance.org), a vendor-neutral group of information security professionals. The CSA is working on a set of best practices as well as information security standards and vendor risk management processes for providers (Crosman, 2010). The CSA has prepared a list of over 200 questions that cover key issues such as data integrity, security architecture, audits, legal/regulatory compliance, governance, and physical security. The IT industry association, CompTIA has recommended that organizations should consider these as resources in evaluating vendors (Olavsrud, 2012).

Some established trade and professional associations have a vested interest in security and privacy issues in the cloud. The American Institute of Certified Public Accountants is making efforts to accelerate cloud adoption among its 350,000 members. The AICPA's resources, expertise and experience would make it easier for it to assess and monitor the performance of cloud vendors, which can help minimize risks for its members. Paychex, a payroll-solutions provider, was the first cloud provider to win the AICPA's official endorsement. The AICPA also endorsed bill.com for invoice management and payment in 2008. In 2009, it endorsed financial management and accounting software maker Intacct and tax-automation supplier Copanion. The AICPA's endorsements are based on an extensive due diligence on the security practices of the vendors (McCann, 2010).

3.2.2. Inter-organizational bodies representing cloud vendors

An inter-organizational system gives the vendors the power of collective action and cooperative endeavor to pursue shared goals which may not be possible if each vendor acts in isolation. A related point is that political processes tend to have a built-in bias that favors organized groups compared to those that are unorganized (Mitra, 1999). Industries such as cloud computing, are likely to benefit from compatibility. For instance, competitive effects associated with compatibility can lead to reduced price and entries of new cloud vendors. Cloud users' decision to switch vendors, however, is likely to be determined by the existing vendor's data-handling policy or their ability to access and delete data with the vendor. Research conducted in other industries indicates that the choice of industry standards is often the result of complex negotiation among industry participants (Farrell, 1987). In the context of this paper, a goal of such negotiation would be to strengthen security and privacy issues and enhance the trustworthiness of this industry (e.g., having an industry-wide secure and trustworthy data-handling policy).

Some argue that industry standards organizations may address many of the user concerns related to privacy and security (Object Management Group, 2009). In the institutional field formed around cloud security, the entry of organizations such as Object Management Group (OMG), the Distributed Management Task Force (DMTF), the Open Grid Forum (OGF), and the Storage Networking Industry Association (SNIA) have led to efforts that are likely to shift the field towards higher security levels because cloud security has been among the top agenda of these organizations (Wittow & Buller, 2010).

A related point is that there are no formal processes for auditing cloud platforms (Vizard, 2010). Analysts argue that auditing standards to assess a service provider's control over data (e.g., SAS

70) or other information security specifications (e.g., the International Organization for Standardization's ISO 27001) are regarded as irrelevant and insufficient to deal with and address the unique security issues facing the cloud (Brodkin, 2010 and gartner.com, 2010). These standards and specifications were not developed specifically for the cloud.

Recent widely publicized security incidents of Epsilon and Amazon Web Services, despite their SAS 70 certification, indicate that that these certifications have provided false assurance to users regarding cloud security. Schroeder (2011, para. 8) comments: “SAS 70 didn't, doesn't, and never will provide assurances for functions such as security and privacy (Epsilon) and security and operational performance (AWS)”. The cloud's disruptive and transformative nature is likely to lead to push for standards that are designed specifically for the cloud industry.

3.3. Cultural-cognitive institutions and their evolution

Cultural-cognitive institutions are “the shared conceptions that constitute the nature of social reality and the frames through which meaning is made” (Scott, 2001, p. 57). Cognitive programs are built on the mental maps of individuals and thus function primarily at the individual level (Huff, 1990). Compliance in cognitive legitimacy concerns is due to habits. Organizations and individuals may not even be aware that they are complying. It is important to consider the effect of the mental maps with respect to the cloud as well as cloud providers.

3.3.1. Perception of vendor's integrity and capability

Cloud computing raises issues related to privacy, security and confidentiality if only for the fact that the users may think that service provider may deliberately or accidentally disclose the data or use for malicious purposes (Ryan, 2011). Of particular concern is thus the users' perception of the dependability of cloud vendors' security assurances and practices. As noted earlier, issues such as confidentiality, integrity, and availability of data related to ineffective or noncompliant controls of service providers, data backup for disaster recovery and third-party backup locations are of concerns to cloud users (Allen, 2011; Table 1). Organizations are also concerned that cloud providers may use insecure ways to delete data once services have been provided (e.g., disposing hard disks without deleting cloud users' data) (Wilshusen, 2010).

The above perceptions are enhanced by the fact that cloud providers allegedly do not answer questions and fail to give enough evidence to trust them (Brodkin, 2010). Businesses and industry analysts are concerned about the cloud providers' so-called “don't ask, don't tell”

approach and have argued that information about data center locations and practices are arguably treated like “national security secrets” (Messmer, 2010).

It is worth noting that malicious insider risks are among the most important risks that the cyberspace faces. According to a report released by the FBI in 2006, over 40% of attacks originate inside an organization (Regan, 2006). While no reported case involving the engagement of a cloud vendor's employee in data breach has yet been found, such risks cannot be ignored. One fear has been that intellectual property and other sensitive information stored in the cloud could be stolen. Worse still, cloud providers may not notify their clients about security breaches. Evidence indicates that many businesses tend to underreport cybercrimes due to embarrassment, concerns related to credibility and reputation damages and fears of stock price drops (Kshetri, 2010). An organization's data in the cloud may be stolen but it may not ever be aware that such incidents had happened.

3.3.2. Cloud users' and providers' inertia effects

Emphasizing the importance of cultural changes in the cloud environment, Microsoft's Dave Coplin recently put the issue this way: Moving into the cloud is a cultural shift as well as a technology shift (Weber, 2011). It is quite possible that organizational inertia may affect the lens through which users view security and privacy issues. Organizational inertia can be defined as formal organizations' tendency to resist internal changes to respond to external changes (Larsen & Lomi, 2002), which may constrain a firm's ability to exploit emerging opportunities (Dean & Meyer, 1996). An inertia effect (resistance to change) is likely to adversely influence organizations' assessment of the cloud from the security and privacy standpoints because they may not be comfortable about losing some of the features of the non-cloud environment such as control on data.

Related to a cultural shift, reduction in control due to the shared and dynamic resources in the cloud environment is a concern. Cloud users have no access to and physical control over the hardware and other resources that store and process their data and information (Wilshusen, 2010). Cloud services contracts, however, often stipulate that data protection is the user's responsibility (Crosman, 2009). A case in point is Google. The company provides security and privacy assurances to its Google Docs users unless the users publish them online or invite collaborators. However, Google service agreements explicitly make it clear that the company provides no warranty or bears no liability for harm in case of Google's negligence to protect the privacy and security (Wittow & Buller, 2010).

Just as important is the need for change in preference for localness. From the standpoint of security, most users tend to prefer computing functions locally on site (Brynjolfsson, Hofmann, & Jordan, 2010). Organizations arguably ask: Who would trust their essential data out there somewhere? (Armbrust et al., 2010).

On the supply side, cultural changes in cloud providers' views towards security practices are also important. A commonplace observation is that while cloud providers offer sophisticated services, their performances have been weak in policies and practices (Wittow and Buller, 2010 and Greengard and Kshetri, 2010). For instance, John Chambers, the Cisco Systems chairman argued that the cloud's security issues cannot be handled in traditional ways as this technology has presented many new and unique challenges (Talbot, 2010).

4. Forces and nature of institutional changes in the cloud industry

4.1. Forces of institutional changes in the cloud industry

They focus on three inter-related issues associated with the cloud: dense networks of actors created by the technology's transformative nature, power dynamics, and contradictions that have emerged with the diffusion of this technology.

4.1.1. Formation of dense networks and relationships in the cloud industry

Prior research indicates that paradigm shifts involve a social learning process that may comprise numerous and diverse participants with broad social and economic demands and interests who want to accomplish multiple purposes that are not always congruent (Baumgartner and Jones, 1993 and Hall, 1993). Unsurprisingly, due to the cloud's dynamic and transformative nature, it is drawing diverse actors. Some of the key actors and interactions among them in the thickening institutional field formed around cloud security are presented in Fig. 1. The attitudes, behavior and expectations of these actors influence the equilibrium of the game in the cloud industry (Snidal, 1996, p. 128).

As noted above, these actors seem to be in the mobilization stage (Purdy & Gray, 2009) and there is a significant trend towards collaboration, coordination and communication among them. The cloud has led to the generation of new interactions among private sector agents (e.g., the CSA and CompTIA). Powerful cloud vendors are also encouraging public–private interactions,

leading the coordination efforts and influencing national and international policy-making processes, which may improve cloud security. In January 2011, Microsoft general counsel spoke to the French National Assembly and urged to lower cloud barriers (O'Brien, 2011). At the event, fueling the European Economy (http://www.microsoft.eu/innovation-in-society/events/event-fueling-the-european-economy.aspx) hosted by Microsoft in Brussels, Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, gave a keynote speech and emphasized that the Commission's proposal would improve privacy and allow for the development and deployment of cloud services (Ashford, 2012).

Kroes also urged cloud providers and users to participate in talks about security and technical/commercial standardization (Thiel & Valpuesta, 2011). At the 2012 World Economic Forum in Davos, Switzerland, the EU announced the European Cloud Partnership, which focuses on the public sector's role. The idea in the partnership is to help make the cloud more appropriate for the public sector and increase the public sector's involvement in the cloud. In a blog (http://blogs.ec.europa.eu/neelie-kroes/european-cloud-partnership/), Kroes noted that cloud vendors, industry bodies and associations such as SAP, Digital Europe, EuroCloud, OpenForum Europe, TechAmerica Europe, and Google reacted positively to the partnership. This is a sign of an increasing level of public–private interaction.

The above activities are indicative of the formation of a dense network of relationships among various actors in the institutional field formed around cloud security, which is likely to reduce incentives for opportunism (Axelrod & Cohen, 2001). Dense relationships and interactions are also likely to generate a lot of gossips, which would help enhance trust. For instance, if formal mechanisms are created to provide trust on the cloud, vendors and users do not have to depend on personal or organizational characteristics or past exchange history. Zucker (1986) refers this phenomenon as institutionally based trust.

4.1.2. The power dynamics in the cloud industry

The various entrepreneurial initiatives and activities that accompany the development of the cloud industry have been highly noticeable and difficult to ignore. In this regard, there is much to learn from policy entrepreneurship, which entails recognizing and promoting an understanding of a political landscape or transforming it in order to create new opportunities (Baumgartner & Jones, 1993).

It is important to develop an adequate description of the relative distribution of power in order to understand the nature of negotiations and interactions among various players. The sources and nature of powers of various key actors are discussed above and presented in Table 2. Here, they mainly focus on power dynamics from the perspective of exchange relationships. Exchange relationships in an industry are influenced by the relative power and dependence of the actors (Emerson, 1962 and Fligstein and Dauter, 2007). What interests them about the current power dynamics between users and providers of cloud is that these actors are helping to move the institutional field around cloud industry closer to the structuration stage.

Dropbox's updates in its terms and conditions in response to user pressures (Table 2) and other similar examples indicate that users' relative power vis-a-vis providers has increased with intense competition. Cloud users are leveraging this increased power to force providers to take measures to enhance privacy and security. Using the term that Kim, Pinkley, and Fragale (2005, p. 810) do, they can say that cloud users have employed power tactics in an attempt to strengthen their power vis-a-vis the providers.

The contracts that involved Google and Computer Sciences Corporation (CSC) with the City of Los Angeles is an example that is illustrative of how traditional contracts between service providers and clients fail to address the legal and structural issues. Over time cloud users are likely to realize how incomplete or vague contracts may expose them to various risks. The increased relative power is likely to enable them to push for contracts that are more detailed and more complete. They may also create intense pressure for a regulatory response that properly addresses security and privacy issues and shift at least some of the legal responsibility from the user to the vendor (Fig. 1).

Cloud vendors, on the other hand, are increasing their capacity to negotiate with and influence the users by offering them new, innovative and potentially attractive value propositions. Put differently, they are attempting to increase their “potential power” (Kim et al., 2005, p. 803). One example is the vendor, HiDrive Free. The company's selling proposition is that its data centers are hosted in Germany, a country with among the strictest privacy laws (Table 2). Cloud providers are thus reacting to a perceived decline in power by engaging in proactive behaviors to develop more secure products.

4.1.3. Contradictions associated with the cloud

A simple approach to understand institutional changes associated with the cloud would be to look at the various contradictions and dilemmas that the cloud produces with the existing institutional arrangements, which are likely to shape decision-making processes of key institutional actors. Institutional theorists view this as accumulated results of organizations' continuous isomorphic adaptations (Burns & Nielsen, 2006). If they look from this viewpoint, institutional changes can be seen as an outcome of the dynamic interactions of contradictions and "praxis" (Seo & Creed, 2002, p. 222). That is, institutional actors continuously engage in the process of enactment, embodiment and interpretation of theories, lessons and skills, which leads to institutional changes.

First, conformance to the existing institutions may be at the expense of technical and functional efficiency, which is likely to act as a force of institutional changes. As noted above, the ETNO has emphasized the importance of changing rules related to online privacy and data transfers, so that European companies can compete on the same level as those in the U.S. (Ingthorsson, 2011). Likewise, the EU is working to develop appropriate regulative framework due to the critical role of the cloud in the economic growth of the member countries (Thiel & Valpuesta, 2011). Seo and Creed (2002, p. 226) refer this type of contradiction as "legitimacy that undermines functional inefficiency".

Service providers respond to the rapidly changing IT environment by making adaptations that help them to maintain competitive advantage in the new technological landscape. The continuous adaptation has resulted in a competency trap whereby IT service providers attempt to pursue cost management programs such as minimizing the total cost of ownership (TCO). Many services providers have shown an inability to adapt to the environment of the cloud, which poses unique security problems. Seo and Creed (2002, p. 226) refer this phenomenon as "adaptation that undermines adaptability" in which "adaptive moves make adopters less able to adapt over the long run". As security and privacy issues are becoming more important, cloud users are demanding an explicit guarantee of data security and liability clauses in contracts with their cloud vendors. Users' pressures to Dropbox to update its terms and conditions regarding data security and ownership can serve as an example to illustrate this point (Table 2).

Third, the legitimacy seeking process may require appeasing multiple institutions that are conflicting and inconsistent. This type of contradiction is referred as "isomorphism that conflicts with divergent interests" which may act as a trigger for institutional change (Seo & Creed, 2002, p. 226). For instance, IT companies such as Oracle, Cisco Systems, SAP, Apple, Google and Microsoft lobbied to streamline EU's fragmented national data protection laws (O'Brien, 2011).

Finally, businesses, industry bodies and government organizations in some countries have achieved some progress towards developing institutions that are more or less compatible with other prevailing institutions in their countries. These intra-national measures are in conflict with the frameworks adopted by other countries. Such inconsistencies are described as “intra-institutional conformity that creates inter-institutional incompatibilities”, which are likely to bring about pressures for changes (Seo & Creed, 2002, p. 226). To take an example, the EU member states are working to align privacy laws and close the existing jurisdictional gaps across the member states.

4.2. The nature of likely changes in cloud related institutions

According to a rational choice perspective, a firm is likely to pursue strategies that maximize its overall profitability. However, when external forces threaten organizations' business models, they are likely to engage in experimentation in a variety of ways (Sosna, Trevinyo-Rodríguez, & Velamuri, 2010) with “changing mix of technological and market conduct” (Antonelli, 1993, p. 625).

Regarding the potential changes in a company's strategies, there is another lesson to be learned from the functioning of a political landscape. In most cases, policy changes are likely to take place only incrementally (Lindbolm, 1959). Moreover, policies changes often happen in a reactive rather than a proactive fashion (Lindblom, 1968). To put things in context, cloud vendors are likely to change their business models and routine strategies in response to various pressures. As noted earlier, the cloud provider, Dropbox, which was forced to update its terms and conditions in response to customers' dissatisfaction with the clause detailing data ownership issues, serves as an illustrative example (Table 2).

In the cloud industry, the vendors are likely to face unprecedented pressure to gain customer trust. The production of trust, however, is a time consuming process. For cloud vendors it requires engagement in exchange processes with the clients and fulfillment of “transactional obligations” (Bailey, Gurak, & Konstan, 2003, p. 312). That is, users' willingness to confer trust on vendors is a function of the latter's history of providing a trustworthy cloud computing resources, services and environment.

5. Discussion and implications

While technological development to address the security concerns is critical, institutional measures such as clearer regulatory frameworks and other trust producing initiatives are no less important. Due to the cloud's transformative and far-reaching impacts and significance, it has drawn diverse actors and participants with different perspectives that have broad social and economic demands and interests. These participants vary widely in resources, expertise, experience and power and their actions are aimed at accomplishing multiple political, social and economic goals, which are far from congruent. In fast developing technologies such as the cloud, the institutional change patterns do not seem to reflect the linearity observed in more mature industry. National governments' and supra-national agencies' roles in the development of cloud related institutions have been mostly passive and reactive rather than active and self-initiated. Since some non-profit organizations and industry bodies as well as various associations representing cloud vendors and users have been relatively active and some of them are also engaged in organized lobbying efforts to influence national/international policy making, it is reasonable to expect that the development of normative institutions is likely to be followed by the development of regulative institutions. As in the case of the internet Domain Name System (DNS), the development of regulative institutions in the cloud industry is likely to be an ex post facto legitimation of a the codification of industry norms.1 It is anticipated that the salience of an institutional component may also vary over time. For instance, barriers associated with newness and inertia effects are likely to decline over time. On the other hand, as the penetration level, width and depth of clouds increase, they may be more attractive cybercrime targets which would mean that the importance of cloud security would further increase.

The above discussion has implications for implications for cloud providers, users and policy makers.

5.1. Implications for cloud providers

Most cloud providers' services come with no assurance or promise of a given level of security and privacy. Nor is that their only problem. Cloud providers have also allegedly demonstrated a tendency to reduce their liability by proposing contracts with the service provided as is with no warranty (McCafferty, 2010). Perception of ineffectiveness or noncompliance of cloud providers may thus act as a roadblock to organizations' cloud adoption decisions. In this regard, security and privacy measures designed to reduce perceived risk as well as transparency and clear communication processes would create a competitive advantage for cloud providers.

Cloud vendors may address many of the user concerns by becoming more transparent. Since regulative institutions related to liability and other issues are not well developed, cloud providers

may feel pressures to obtain endorsements from professional societies. AICPA's endorsements have driven the diffusion of cloud applications among some CPA firms.

5.2. Implications for cloud users

The newness and uniqueness of the cloud often mean that clients would not know what to ask for in investment decisions. Most users are functioning on the assumption that cloud providers possess a reasonable capability and are willing to protect privacy and security of their data (Wittow & Buller, 2010). However, against the backdrop of the current institutional and technological contexts, this assumption may not always be realistic. Given the institutional environment, potential adopters may need to ask tough questions to vendors regarding certification from auditing and professional organizations, data center locations, and background checks of employees.

The above analysis suggests that a one-size-fits-all approach may not work for all user organizations' cloud adoption. For instance, organizations may have to make decisions concerning combinations of public and private clouds. A public cloud is effective for an organization handling high-transaction/low-security or low data value (e.g., sales force automation). Private cloud model, on the other hand, may be appropriate for enterprises and applications that face significant risk from information exposure such as financial institutions and health care provider or federal agency. For instance, for medical-practice companies dealing with sensitive patient data, which are required to comply with the HIPAA rules, private cloud may be appropriate.

Other issues of particular relevance and concern for cloud users are government overreach and the cloud's potential to be the ultimate spying machine. There are stories of espionage activities' successful transition to cyber-espionage2.0 and national and international security issues. A Google's report released in April 2010 is especially timely and enlightening. The company described how government authorities around the world request the company for private information and to censor its applications.

There have been concerns about possible overreach by law enforcement agencies. In the U.S., for instance, thanks to the 2001 Patriot Act, the federal government can ask service providers for details of a user's activities without telling the user. The FBI's audits indicated the possibility of overreach by the agency in accessing internet users' information (Zittrain, 2009).

For some analysts, the biggest concern has been the government's increased ability to access business and consumer data, and a lack of constitutional protections against these actions (Talbot, 2010). Especially, the cloud is likely to provide authoritarian regimes a fertile ground for cyber-control and spying activities.

5.3. Implications for policy makers

Since geographic dispersion of data is an important factor associated with cost and performance of the cloud, an issue that deserves mention relates to regulatory arbitrage, which means that cloud vendors can take advantage of loopholes in regulatory systems of certain jurisdictions to reduce risks. Economies worldwide vary greatly in the legal systems. Experts expect that, at least for the short run, countries are likely to update their laws individually rather than acting in a multilateral fashion (TR, 2010). Due to the newness, jurisdictional arbitrage is higher for the cloud compared to the IT industry in general. In this regard critics are concerned that cloud providers may store sensitive information in jurisdictions that have weak laws related to privacy, protection and availability of data (Edwards, 2009). Given the cloud's significance to economic competitiveness and national security, policy makers need to look at developments in cloud-related institutions in other countries and take proactive measures to enact and enforce laws for developing the cloud industry.

5.4. Future research

Before concluding, several potentially fruitful avenues for future research are suggested. Cloud-related institutions are currently thin and dysfunctional. As noted above, privacy and security issues of in the cloud currently fall into a legally gray area. Future research might examine how political, ethical, social and cultural factors are associated with security issues in cloud computing.

As noted above, prior research has suggested that building a regulative/law pillar system is the first stage of field formation. It is followed by a formation of normative institutions and then cognitive institutions (Hoffman, 1999). In this regard, a comparison of the nature of institutional evolution in the cloud industry with those in other economic sectors might be worthwhile target of study.

Second, an empirical examination of core premises of this paper would be useful for studying the institutional drivers of the cloud industry. Such a study would shed light on the relative importance of various factors discussed above in organizations' cloud adoption decision.

Finally, future research might also explore antecedents of organizations' cloud computing decisions in terms of various technological dimensions identified in the prior literature. One avenue would be to test how the cloud performs in terms of major dimensions proposed by Rogers (1995) such as relative advantage, compatibility, complexity, observability and trialability.

6. Concluding comments

The cloud's vast storage capabilities and availability of an array of contents and applications also poses monumental risks related to privacy and security. This issue is very significant for cloud diffusion as organizations are using the cloud to perform increasingly strategic and mission critical functions. At the same time, cloud providers are facing pressures and challenges to protect information assets belonging to their customers and other sensitive data. A related point is that there is currently a big gap between what cloud vendors claim and what the existing and potential adopters think about the cloud's security. On the plus side, industry players are realizing a need to develop standards to provide the guidance necessary for security and privacy. As a result of various organized and individual efforts, positive changes in cloud-related institutions can be anticipated.

Cloud users are becoming educated and are bringing more holistic perspectives to incorporate all the relevant issues that are important to them such as cost saving, productivity gain, security and privacy issues and, voice and control over data. They have also changed their behavior in response to changing perceptions of benefits and risks and their potential and realized power. Over time, this may give venders a better assessment of clients' needs and power, which may lead to an effective tailoring of services and improvements in security.

Nation states and international actors are also facing unprecedented demands, challenges and pressures to introduce new regulations, change the existing regulations and in some cases, close loopholes in the existing regulations. They hope that these measures would help enhance national security as well as security/privacy of user data, increase national competitiveness in technology and facilitate cloud adoption by consumers and organizations.

Acknowledgment

An earlier version of this paper was presented at the Pacific Telecommunication Council's 2011 annual conference held in Honolulu, Hawaii (January 16–19, 2011). Two anonymous reviewers' comments on earlier versions helped to improve the paper substantially.

References

J.M. Allen. Cloud computing: Heavenly solution or pie in the sky? Pennsylvania CPA Journal, 82 (1) (2011), pp. 1–4.

C. Antonelli. Investment and adoption in advanced telecommunications. Journal of Economic Behavior and Organizations, 20 (1993), pp. 227–245.

M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski et al. A view of cloud computing. Communications of the ACM, 53 (4) (2010), pp. 50–58.

Ashford, W. (2012, January 31). Proposed EC data protection rules help cloud adoption. Retrieved from (http://www.computerweekly.com/news/2240114617/Proposed-EC-data-protection-rules-help-cloud-adoption-says-Kroes).

R. Axelrod, M.D. Cohen. Harnessing complexity: Organizational implications of a scientific frontier. Basic Books, New York (2001).

J.F. Backoff, C.L. Martin Jr. Historical perspectives: Development of the codes of ethics in the legal, medical and accounting professions. Journal of Business Ethics, 10 (1991), pp. 99–110.

B.P. Bailey, L.J. Gurak, J.A. Konstan. Trust in cyberspace. J. Ratner (Ed.), Human factors and web development (2nd ed.), L. Erlbaum Associates Inc, Hillsdale, NJ, USA (2003), pp. 311–321.

W.P. Barnett, G.R. Carroll. How institutional constraints affected the organization of early US telephonies. Journal of Law, Economics and Organization, 9 (1993), pp. 98–126.

F.R. Baumgartner, B.D. Jones. Agendas and instability in American politics. University of Chicago Press, Chicago (1993).

Bradley, T. (2010). Build your own private azure cloud with new Microsoft appliance. PC World. Retrieved from (http://www.pcworld.com/businesscenter/article/200988/build_your_own_private_azure_clouc_with_new_microsoft_appliance.html?tk=hp_blg).

S. Bradner. Internet privacy conflicts. Network World, 27 (18) (2010), p. 15.

J. Brodkin. 5 problems with SaaS security. Network World, 27 (18) (2010), pp. 1–27.

E. Brynjolfsson, P. Hofmann, J. Jordan. Cloud computing and electricity: Beyond the utility model. Communications of the ACM, 53 (5) (2010), pp. 32–34.

J. Burns, K. Nielsen. How do embedded agents engage in institutional change? Journal of Economic Issues, 40 (2) (2006), pp. 449–456.

J.L. Campbell. Institutional change and globalization. Princeton University Press, Princeton, NJ (2004).

J.R. Cohen, L.W. Pant. Beyond bean counting: Establishing high ethical standards in the accounting profession. Journal of Business Ethics, 10 (1991), pp. 45–46.

Cooter, M. (2011). Strato launches competitor to Dropbox— with added privacy. Retrieved from (http://www.cloudpro.co.uk/iaas/cloud-storage/1641/strato-launches-competitor-dropbox-added-privacy).

M. Covaleski, M. Dirsmith. An institutional perspective on the rise, social transformation and fall of a university budget category. Administrative Science Quarterly, 33 (1988), pp. 562–587.

P. Crosman. Securing the clouds. Wall Street & Technology, December (2009), p. 23.

T.J. Dean, G.D. Meyer. Industry environments and new venture formations in U.S. manufacturing: A conceptual and empirical analysis of demand determinations. Journal of Business Venturing, 11 (1996), pp. 107–132.

M. Dickson, R. BeShers, V. Gupta. The impact of societal culture and industry on organizational culture: Theoretical explanations. J.H. Robert, J.H. Paul, J. Mansour, W.D. Peter, G. Vipin (Eds.), Culture, leadership, and organizations: The GLOBE study of 2 societies, Sage Publications, Thousand Oaks, CA (2004).

J. Edwards. Cutting through the fog of cloud security. Computerworld, 43 (8) (2009), pp. 26–29.

Ely, A. (2011, March 7). 5 Steps to secure SaaS. Information Week, p. 17, (http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=229300176).

R.M. Emerson. Power-dependence relations. American Sociological Review, 27 (1962), pp. 31–40.

European Commission (2010). The future of cloud computing—Opportunities for European cloud computing beyond. Retrieved from (http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=6993).

J. Farrell. Cheap talk, coordination, and entry. The RAND Journal of Economics, 18 (1) (1987), pp. 34–39.

N. Fligstein, L. Dauter. The sociology of markets. Annual Review of Sociology, 33 (1) (2007), pp. 105–128.

gartner.com (2010, July 14). Gartner says SAS 70 is not proof of security, continuity or privacy compliance. Retrieved from (http://www.gartner.com/it/page.jsp?id=1400813).

M.A. Goodburn, S. Hill. The cloud transforms business. Financial Executive, 26 (10) (2011), pp. 34–39.

S. Greengard, N. Kshetri. Cloud computing and developing nations. Communications of the ACM, 53 (5) (2010), pp. 18–20.

R. Greenwood, C.R. Hinings. Understanding radical organizational change: Bringing together the old and the new institutionalism. Academy of Management Review, 21 (1996), pp. 1022–1054.

P. Hall. Policy paradigms, social learning, and the state: The case of economic policymaking in Britain. Comparative Politics, 25 (1993), pp. 275–296.

L. Henkin. How nations behave. Council on Foreign Relations, New York (1979).

A.J. Hoffman. Institutional evolution and change: Environmentalism and the US chemical industry. Academy of Management Journal, 42 (4) (1999), pp. 351–371.

A.S. Huff. Mapping strategic thought. A.S. Huff (Ed.), Mapping strategic thought, Wiley, Chichester, England (1990).

Ingthorsson, O. (2011, August 29).Regulations a barrier to cloud growth in Europe. Retrieved from (http://www.datacenterknowledge.com/archives/2011/08/29/enhancing-cloud-development-in-europe/).

N.K. Katyal. Criminal law in cyberspace. University of Pennsylvania Law Review, 149 (4) (2001), pp. 1003–1114.

P.H. Kim, R.L. Pinkley, A.R. Fragale. Power dynamics in negotiation. Academy of Management Review, 30 (4) (2005), pp. 799–822.

N. Kshetri. The global cyber-crime industry: economic, institutional and strategic perspectives. Springer-Verlag, Heidelberg (2010).

N. Kshetri, N. Dholakia. Professional and trade associations in a nascent and formative sector of a developing economy: A case study of the NASSCOM effect on the Indian offshoring industry. Journal of International Management, 15 (2) (2009), pp. 225–239.

E. Larkin. Will cloud computing kill privacy? PC World, 28 (3) (2010), p. 44.

E. Larsen, A. Lomi. Representing change: A system model of organizational inertia and capabilities as dynamic accumulation processes. Simulation Model Practice and Theory, 10 (5) (2002), pp. 271–296.

C.E. Lindblom. The policymaking process. Prentice-Hall, Englewood Cliffs, NJ (1968).

C.E. Lindbolm. The science of "muddling through." Public Administration Review, 19 (1959), pp. 79–88.

D. McCafferty. Cloudy skies: public versus private option still up in the air. Baseline, 103 (2010), pp. 28–33.

McCann, D. (2010). Posted in: accountants head to the cloud, CFO.com. Retrieved from (http://cfo.com/article.cfm/14484960/c_14485112?f=home_todayinfinance).

L. McCreary. What was privacy? Harvard Business Review, 86 (10) (2008), pp. 123–131.
Messmer, E. (2010). Secrecy of cloud computing providers raises IT security risks. Retrieved from (http://www.mis-asia.com/news/articles/secrecy-of-cloud-computing-providers-raises-it-security-risks).

D. Mitra. Endogenous lobby formation and endogenous protection: A long-run model of trade policy determination. American Economic Review, 89 (5) (1999), pp. 1116–1134.

K.L. Newman. Organizational transformation during institutional upheaval. The Academy of Management Review, 25 (3) (2000), pp. 602–619.

Nguyen, A. (2011, September 7), Only seven percent of UK it services in the cloud, says survey, Computerworld. Retrieved from (http://www.itworld.com/cloud-computing/200657/only-seven-percent-uk-it-services-cloud-says-survey).

D.C. North. Institutions, institutional change and economic performance. Cambridge University Press, Cambridge, UK (1990).

D.C. North. Epilogue: Economic performance through time. L.J. Alston, T. Eggertsson, D.C. North (Eds.), Empirical studies in institutional change, Cambridge University Press, Cambridge, PA (1996).

NW (Network World). (2010). Inside the cloud security risk, 27(13), 11.

Object Management Group. (2009). Cloud-standards.org, Major standards development organizations collaborate to further adoption of cloud standards. Retrieved from (http://www.omg.org/news/releases/pr2009/07-13-09.htm).

O'Brien, K. J. (2011, July 24). Europe turns to the cloud. Retrieved from (http://www.nytimes.com/2011/07/25/technology/europe-turns-to-the-cloud.html?pagewanted=all).

Olavsrud, T. (2012, February 18). Security in the cloud is all about visibility and control. Retrieved from (http://www.cso.com.au/article/415872/security_cloud_all_about_visibility_control/).

M. Price. Pinning down the cloud. The Wall Street Journal (2011), p. R3.

J.M. Purdy, B. Gray. Conflicting logics, mechanisms of diffusion, and multilevel dynamics in emerging institutional fields. Academy of Management Journal., 52 (2) (2009), pp. 355–380.

R. Reay, K. Golden-Biddle, K. GermAnn. Legitimizing a new role: Small wins and microprocesses of change. Academy of Management Journal, 49 (2006), pp. 977–998.

Regan, K. (2006). FBI: cybercrime causes financial pain for many businesses, technewsworld. Retrieved from (http://www.technewsworld.com/story/48417.html).

Ricadela, A. (2011, September 1). Cloud security is looking overcast. Retrieved from (http://www.businessweek.com/magazine/cloud-security-is-looking-overcast-09012011.html).

E.M. Rogers. Diffusion of innovations. (4th ed.)Free Press, New York (1995)

Russell, J. (2011, June 25), China to develop $154m tech centre free of web restrictions. Retrieved from (http://asiancorrespondent.com/58249/china-to-develop-154m-tech-centre-free-of-web-restrictions/).

M.D. Ryan. Cloud computing privacy concerns on our doorstep. Communications of the ACM, 54 (1) (2011), pp. 36–38.

SAS 70 Overview, (2011). Retrieved from (http://sas70.com/sas70_overview.html).

Schroeder, D. (2011, July 5), SAS 70 Is dead: Hello better cloud governance?. Retrieved from (http://www.informationweek.com/news/global-cio/compliance/231000966).

J.A. Schumpeter. Business cycles: A theoretical, historical and statistical analysis of the capitalist process. McGraw-Hill, New York and London (1939).

R. Scott. Institutions and organizations. Sage, Thousand Oaks, CA (1995). R. Scott. Institutions and organizations. Sage, Thousand Oaks, CA (2001).

W.R. Scott, M. Ruef, P.J. Mendel, C.A. Caronna. Institutional change and healthcare organizations: From professional dominance to managed care. University of Chicago Press, Chicago, IL (2000).

M.G. Seo, W.E.D. Creed. Institutional contradictions, praxis, and institutional change: A dialectical perspective. Academy of Management Review, 27 (2) (2002), pp. 222–247.

J. Smith, D. Wiest. The uneven geography of global civil society: National and global influences on transnational association. Social Forces, 84 (2) (2005), pp. 621–651.

D. Snidal. Political economy and international institutions. International Review of Law and Economics, 16 (1) (1996), pp. 121–137.

M. Sosna, R.N. Trevinyo-Rodríguez, S.R. Velamuri. Business model innovation through trial-and-error learning: The naturhouse case. Long Range Planning, 43 (2-3) (2010), pp. 383–407.

D. Talbot. Security in the ether. Technology Review, 113 (1) (2010), pp. 36–42.

Thiel, S., & Valpuesta, R., (2011, September 13). U.K. Trails U.S. in public cloud adoption, Sales force CEO Says. Retrieved from (http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/09/13/bloomberg1376-LRILRH0YHQ0×01-3L8HOVDU01DK87C6RGOVTSL63E.DTL).

Tillery, S. (2010). How safe is the cloud? Retrieved from (http://www.baselinemag.com/c/a/Security/How-Safe-Is-the-Cloud-273226).

TR (Telecommunications Reports). (2010). Microsoft urges policymakers to help secure cloud computing, 76(3), 18-19.

Vizard, M. (2010). Assessing the risks of cloud computing. Retrieved from (http://www.itbusinessedge.com/cm/blogs/vizard/assessing-the-risks-of-cloud-computing/?cs=43712).

Weber, T. (2011). Cloud computing: How to get your business ready. Retrieved from (http://www.bbc.co.uk/news/business-12779201).

L.L. Whitcomb, C.B. Erdener, Cheng Li. Business ethical values in China and the U.S. Journal of Business Ethics, 17 (8) (1998), pp. 839–852.

G.C. Wilshusen. Information security federal guidance needed to address control issues with implementing cloud computing. GAO Reports, preceding (2010), pp. 1–48.

M.H. Wittow, D.J. Buller. Cloud computing: Emerging legal issues for access to data, anywhere, anytime. Journal of Internet Law, 14 (1) (2010), pp. 1–10.

Worth, D. (2011, June 16), European Parliament calls for stronger data protection rules. Retrieved from (http://www.v3.co.uk/v3-uk/news/2079420/european-parliament-calls-stonger-protection-rules).

D. Zielinski. Be clear on cloud computing contracts. HRMagazine, 54 (11) (2009), pp. 63–65.

J. Zittrain. Lost in the cloud. The New York Times (2009), p. A 19.

L. Zucker. Production of trust: Institutional sources of economic structure 1840–1920. Research in Organizational Behaviour, 8 (1986), pp. 3–11.