nccr trade regulation
swiss national centre of competence in research

Working Paper No 2013/23 I AUGUST 2013

Governments and Cloud Computing: Roles, Approaches, and Policy Considerations

URS GASSER and DAVID R. O'BRIEN

Governments from Bogota to Beijing are engaging with emerging cloud computing technologies and its industry in a variety of overlapping contexts. Based on a review of a representative number of advanced cloud computing strategies developed by governments from around the world, including the United States, United Kingdom, the European Union, and Japan, we observed that these governments – mostly implicitly – have taken on several different "roles" with respect to their approaches to cloud computing. In particular, we identify six distinguishable but overlapping roles assumed by governments: users, regulators, coordinators, promoters, researchers, and service providers. In this paper, we describe and discuss each of these roles in detail using examples from our review of cloud strategies, and share high-level observations about the roles as well as the contexts in which they arise. The paper concludes with a set of considerations for policymakers to take into account when developing approaches to the rapidly evolving cloud computing technologies and industry.

FNSNF
FONDS NATIONAL SUISSE
SCHWEIZERISCHER NATIONALFONDS
FONDO NAZIONALE SVIZZERO
SWISS NATIONAL SCIENCE FOUNDATION

Die Nationalen Forschungsschwerpunkte (NFS) sind ein Förderinstrument des Schweizerischen Nationalfonds.
Les Pôles de recherche nationaux (PRN) sont un instrument d'encouragement du Fonds national suisse.
The National Centres of Competence in Research (NCCR) are a research instrument of the Swiss National Science Fondation.

Governments and Cloud Computing: Roles, Approaches, and Policy Considerations*

Urs Gasser & David R. O'Brien†

Contents

* This paper synthesizes findings from a multi-year cloud computing research initiative led by the Berkman Center, in close collaboration with the Nexa Center for Internet & Society (Italy), Keio University (Japan), the Research Center for Information Law (Switzerland), and the NCCR Trade Regulation (Switzerland), and the participants at our Cloud Computing Workshop series held in Cambridge, MA, Washington, DC, and Keio University in Japan.
† Urs Gasser is the Executive Director of the Berkman Center for Internet & Society and Professor of Practice at Harvard Law School; David O'Brien is a Senior Project Coordinator at the Berkman Center. The authors wish to thank Herbert Burkert, Mira Burri, Catharina Maracke, Juan Carlos de Martin, and the members of the cloud research team at the Berkman Center, including Oliver Goodenough and summer interns Takumi Shimizu, Jef Ausloos, Keisuke Otsubo, Liz Woolery, and Sanna Kulvska, for research assistance, support, and feedback. Special thanks to Caroline Nolan for her many substantive contributions. Comments are welcome at ugasser@cyber.law.harvard.edu and dobrien@cyber.law.harvard.edu.

I. Introduction

In recent years, cloud computing – a term that broadly describes an emerging group of related technologies and business models[i] – has become standard vocabulary for Chief Information Officers in the private and public sectors who wish to harness the potential benefits of this technology for their organizations and businesses. Simultaneously, it has grabbed the attention of policymakers and public officials, who are charged with creating a thriving, sustainable information and communication technology ecosystem for the future.

The most visible expression of the growing government engagement with cloud technologies and companies are the high-level cloud strategies being developed and implemented by a number of nations around the world.

The US government's "Federal Cloud Computing Strategy" is a particularly rich example of a comprehensive strategy that involves multiple levels of government. In an extensive effort to reduce costs and increase efficiency, the strategy set in motion a mandatory transition of older government IT systems to cloud computing technologies.[ii] Similarly, Japan's "Smart Cloud Strategy" sets forth a high-level plan to "maximize the use of cloud services," "promote the widespread use of ICT," and "amass and share a wealth of information and knowledge beyond the boundaries of companies and industries across the entire social system" with an eye towards creating "new economic growth" and "bolstering Japan's international competitiveness."[iii] European countries are also pursuing cloud strategies. At the highest level, the European Commission (EC) stated its commitment to cloud computing and a long-term plan for propagating a common set of rules aimed at fostering a cohesive market structure among the EU member states for cloud service providers.[iv] The European Commission's strategy seeks to enable faster adoption in both the public and private sectors, which it hopes will increase productivity, economic efficiency, and create new jobs across the European Economic Area.[v] The strategy includes plans to address potential issues that would impede adoption and use through policy measures.[vi]

The strategies noted above, and in others that will discussed in the paper, provide a lens for understanding how governments[vii] currently *perceive* cloud computing and how they are beginning to react to its emergence. For the purpose of this paper, a research team at the Berkman Center for Internet & Society at Harvard University has reviewed a representative number of advanced cloud strategies from different parts of the world – including, among others, the United States, United Kingdom, European Union, and Japan – in order to identify and discuss the roles that governments have assumed in their approaches to cloud computing, as well as the tools they employ to reach their goals, and to highlight key factors and issues for policymakers to consider as they develop approaches to the cloud.

One of the findings from this review of cloud strategies is that governments – mostly implicitly – have taken on *several different roles* with respect to their approaches to cloud computing. Although these categories have overlapping characteristics, one can analytically distinguish among six basic (or ideal-type) roles:

- *Governments as Users* – governments are adopting cloud computing services to take advantage of its costs savings and innovative features
- *Governments as Regulators* – acting through their legislative, judicial, regulatory branches, governments regulate to implement policy through the rule of law
- *Governments as Coordinators* – governments coordinate public and private initiatives, through standard setting processes, and by facilitating the sharing of information between private and public stakeholders
- *Governments as Promoters* – governments actively promoting the cloud industry by endorsement, funding, and incubation programs
- *Governments as Researchers* – governments conducting or funding research on technical or societal issues related to cloud computing
- *Governments as Service Providers* – governments providing cloud services for use by other government agencies or the public

In the following sections, we discuss each role in greater detail by using examples from our international review of cloud strategies. In this context, we share high-level observations and address selected policy issues within the respective roles (II). Next, we share some observations about the approaches and tools used within each role, as well as the overall contextual positioning of the roles (III). The paper concludes with a set of considerations for policymakers engaged in cloud issues (IV).

II. Roles of Governments and Related Activities

1. Government as a User

1.1 Overview and Examples

Governments are replacing their legacy IT systems with cloud computing technologies and implementing new cloud-based tools for collaboration and information sharing across agencies and units. Whether working with third-party vendors, building massive private data centers maintained by government employees, or using hybrid clouds, governments are in this sense *users* of cloud computing, much in the same way that a consumer is a user of cloud computing services.

While some governments we surveyed are implementing cloud computing in an *ad hoc* fashion (for example, by outsourcing an agency's email service absent wider coordination across governmental entities), others are in the process of implementing highly coordinated and large-scale strategies aimed at further governmental adoption and use of cloud technologies.

The following cloud initiatives are among the most advanced strategies we reviewed:

(a) United States

The US federal government's 2010 plan to shift a significant fraction of its current IT resources to cloud computing technologies has been organized and coordinated by the US Chief

Information Officer (CIO) at the Office of Management and Budget (OMB) and the US CIO Council, which consists of CIOs from major agencies,[viii] with special support from the National Institute for Standards and Technology (NIST), General Services Administration (GSA), and the Department of Homeland Security (DHS). While a highly coordinated effort, the US agencies are individually responsible for developing, implementing, and reporting the status of the strategy milestones set by the US CIO and CIO Council. A critical component of the strategy is the "cloud first" policy, a top-down requirement for all executive branch agencies to transition three legacy IT assets to cloud computing within an eighteen month period.[ix] The policy also mandates that, for purposes of future procurement, agencies must evaluate cloud computing options *before* they can acquire off-the-shelf software products. To support migration under the policy, NIST, the GSA, and DHS have worked to identify strategic priorities, issues and challenges that may inhibit migration, served as technical advisors, and have published guidelines for agencies.[x] In addition to addressing the needs of the agencies and departments, the federal government hopes these activities will contribute to similar reform efforts ongoing at the state and local levels of government across the US.

(b) European Union

The European Commission has long been interested in the cloud computing industry, conducting public consultations as early as 2011 and as participants in earlier debates regarding the costs and benefits of cloud technologies.[xi] In 2012 the European Commission announced its commitment to embracing cloud computing through a comprehensive strategy that lays out a framework for conducting research and exploring policy options to accommodate cloud computing across the EU.[xii] The strategy seeks to establish a common set of rules to develop a cohesive market structure among the EU member states for cloud service providers. Although the European Commission's strategy does not immediately foresee the creation of a "European Super Cloud" – a dedicated cloud system for use across Europe in the public sector – one aim of the strategy is to ready the cloud market for public sector use.[xiii] More specifically, the strategy states the EU policies will focus on "enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy which can cut ICT costs, and when combined with new digital business practices, can boost productivity, growth and jobs."[xiv] As part of the effort, the European Commission plans to address several key areas related to harmonizing laws across borders, consumer protection, contracts and transactional fairness, and standards development.[xv]

(c) United Kingdom

Much like the US government, the UK government has been implementing a large-scale reform effort since March 2011 aimed at solving IT problems such as overcapacity, wasteful duplication of resources and systems, insufficient integration and central control, interoperability, and long and costly procurement processes.[xvi] The UK government's larger "ICT Reform Strategy" has four critical components, aimed at delivering cost savings while improving governmental capabilities: G-Cloud, Public Services Network, Data Centre Consolidation, and End User Device Programme.[xvii] Each of these strategies is aimed at improving the operational aspects of government IT both for the benefit of government employees and the public at large. One prominent arm of the overall effort is the "Government Cloud Strategy," which in October 2011 introduced a high-level visions, objectives, and implementation strategy for the UK's "G-Cloud."

The G-Cloud strategy envisions the government developing a policy around governmental use of cloud computing, followed by a widespread initiative to replace and supplement legacy software systems with multi-tenant, shared cloud computing services.[xviii] An evaluation of the first year of the overall reform effort was published in May 2012, according to which the UK government has met many of its early strategy milestones.[xix]

(d) Japan

Japan's Ministry of Internal Affairs and Communications (MIC) and the Ministry for Economy, Trade & Industry (METI) launched the "Smart Cloud Strategy" in May 2010. This initiative aims to "maximize the use of cloud services," "promote the widespread use of ICT," and "amass and share a wealth of information and knowledge beyond the boundaries of companies and industries across the entire social system" with an eye towards creating "new economic growth" and "bolstering Japan's international competitiveness."[xx] To achieve these objectives, MIC and METI are employing three targeted strategies: (1) a utilization strategy, which seeks to promote the use and application of cloud services, (2) a technical strategy, which seeks to promote strategic research and development for next generation cloud services, and (3) a global strategy, which seeks to promote international consensus and global cooperation.[xxi]

1.2 Analysis and Discussion

(a) Benefits

One of the standard questions when discussing the role of governments as users is about the benefits of cloud computing. The brief overview of selected government-led cloud initiatives in the US, Europe, and Asia already indicates that the motivations for cloud adoption and promotion by the public sector are driven by a variety of factors. In our review, we have observed that governments frequently identify the following rationales for adopting cloud computing.

Long-term cost savings: A primary driver governments becoming cloud computing adopters and users is the potential cost savings. Though estimates vary, the US government hopes its shift to cloud computing will eventually save around $5-12 billion in IT spend per year.[xxii] Likewise, the UK government projects that its G-Cloud strategy will save approximately £20M during 2012-2013, £40M during 2013-2014, and £120M during 2014-2015.[xxiii] IT assets will be used more efficiently and easily scaled, reducing upfront capital expenditures associated with traditional infrastructure investments. Cloud services also promise that operational costs will be lower over time as fewer IT staff systems are needed.[xxiv] However, it is worth noting that some commentators have criticized the cost savings projections as being unrealistic.[xxv]

Collaborative and flexible working environments: Many cloud computing services offer available-from-anywhere accessibility and can allow new means of collaboration. For instance, workers can easily access files remotely from laptops, tablets, and smart phones while traveling. They can also work in the same documents at the same time, reducing problems associated with version control. The US and UK strategies, to give two examples,

both emphasize these characteristics in their strategies, noting that cloud computing will allow it to "more easily exploit and share commodity ICT products and services" and enable "the move from high-cost customised ICT applications and solutions to low cost, standard, interchangeable services where quality and cost is driven by the market."[xxvi] Japan, finally, sees the cloud industry as an enabler of domestic and global collaboration, and a means for administering disaster relief.[xxvii]

Encourages long-term innovation: Cloud computing is not only an innovative technology, but also an innovation-enabling technology – a platform that enablers its users to build novel inventions atop basic cloud computing services. In addition to the flexibility and cost savings, this characteristic is often cited in government strategies as factor in support of adoption. The US believes the use of cloud systems promise long-term innovation, as it connects the government with leading technological developments. In addition, cloud computing provides the ability to scale services up and down with agility, which affords the government flexibility for in making decisions regarding IT procurement.[xxviii]

Fosters domestic and international trade: The European Commission is looking to encourage cloud industry growth across the EU by "enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy which can cut ICT costs, and when combined with new digital business practices, can boost productivity, growth and jobs."[xxix] The European Commission estimates that the cloud will contribute €250 billion to the EU in GDP and 3.8 million jobs.[xxx] Japan sees the cloud as a global competition enabler and a way to promote new economic growth.[xxxi] The UK government sees the cloud as a stimulator for its domestic SME market, and gives preference to companies of this size in awarding procurement contracts.[xxxii]

(b) Risks

Taking these benefits at face value, cloud computing has a number of risky characteristics that raise concerns from governments adopting these technologies. According to the US Government Accountability Office (GAO), which audits spending and performance of government agencies, "22 of 24 major federal agencies reported that they were either concerned or very concerned about the potential information security risks associated with cloud computing."[xxxiii] Also topping the list of concerns is "being dependent on the security practices and assurances of vendors" and the use of shared computing resources.[xxxiv] European governments are also concerned about the level of security that cloud computing can provide. The European Commission cautions that "the take up of the cloud by the public sector is subject to the same concerns as seen amongst large private organizations . . . [including,] how can data be made safe in the cloud (as regards confidentiality, integrity, and availability)."[xxxv] A recent report by the European Network of Information and Security Agency (ENISA), which advises the EU on matters related to information security, echoes these concerns noting that the major security issues include loss of governance and control, isolation failures in shared computing resources, insecure and complete data destruction practices, and malicious insiders.[xxxvi]

The underlying architectural characteristics of cloud computing trigger these concerns, in combination with the sensitivity of the information being processed, used, and stored in the cloud as well as and the degree to which the services being provided are critical to the government's operation. These same characteristics are prevalent risk factors to private consumers and organizations that use cloud computing services as well.

Cloud computing services are typically deployed in one of three ways: as a public service, a private service, or a hybrid service.[xxxvii] When deployed *publicly*, a third-party (i.e., non-governmental) cloud service provider provisions cloud computing services to the public at large (i.e., consumers, government, businesses, etc) from infrastructure that the service provider privately owns and operates. In this context, the users of a public cloud service share the same hardware infrastructure (e.g., server arrays, processing power, and storage space) separated by virtual walls. In the *private* cloud deployment model, cloud services are provisioned for use exclusively on infrastructure that is not shared by others. The infrastructure can be owned and operated by a private service provider – sometimes likened to "outsourcing" – or by the user of the cloud services. When deployed in the *hybrid* model, a cloud computing service is provisioned across infrastructure that is both privately and publicly deployed, sometimes across multiple service providers.

Depending on the model in question, it is these characteristics that give rise to the concerns of governments related to security, privacy, and reliability. The tradeoffs between these different models often hinge on the level of control over physical infrastructure and data, cost structures, accessibility and public visibility, and security. Generally speaking, a privately deployed cloud service on government-owned infrastructure will give the government more control over access and security, but will be more expensive to operate and maintain, requiring expensive hardware and a dedicated IT staff.[xxxviii] In contrast, public cloud services are acknowledged to be far less expensive, playing off service providers' economies of scale, broad accessibility, staff expertise, and on-demand scalability. In cases where the cloud service is being provided or operated by a private company, the government must also take into account the companies' overall security and trustworthiness. This might include, for example, the geographic location of the company's facilities, the physical premises on which the service infrastructure resides, the company's personnel, as well as the company's information security practices used on its services and infrastructure. The practical challenges of these risky characteristics and others will be explored in greater detail in the following subsection.

(c) Challenges and Obstacles to Adoption

As noted in the previous subsection, the architecture of cloud computing models portend a number of risks. Governments that are rapidly becoming users of cloud computing services are experiencing a number of challenges as they develop and implement strategies aimed at government adoption, ranging across internally governing major IT transitions, difficulties in scaling procurement, cultural barriers, and challenges with the technology.

Internal Governance and Organizational Complexity

Large-scale cloud projects, such as those ongoing in the US and the UK, can present substantial managerial challenges for those overseeing both the period of transition to cloud services and the complex web of third-party vendors, procurement contracts, governmental decision makers, and IT staff that emerge after implementation. Complicating matters further is that many governments encounter cultural opposition to implementing cloud strategies. Strong planning and management is a prerequisite to handling these issues. However, based on the cases we studied, flexibility and the capacity to adapt is crucial, as even the best-laid plans encounter problems.

In 2012, when examining the progress of US agencies, the US GAO found that the strategic plans for migrating legacy IT assets to cloud services submitted by agencies were "missing one or more key required elements."[xxxix] Of 20 plans evaluated, "only 1 plan fully met the key elements as required."[xl] The GAO found that the remainder of agency plans were not adequate for preparing the agencies to migrate their legacy IT services. Moreover, a substantial portion of agencies evaluated by the GAO have had difficulties implementing the actual system migrations during the first eighteen months of the Cloud First strategy.[xli] The GAO cautioned that the planning and coordination is "essential in determining whether their activities constitute a positive return on investment and therefore, whether the benefits of their activities will be fully realized."[xlii] More recent reports by the US GAO indicate that high-level oversight continues to be an issue in realizing many of the promises of cloud computing.[xliii] Governments in Europe have indicated similar concerns, noting that "the take up of the cloud by the public sector is subject to the same concerns as seen amongst large private organizations . . . [including,] how to manage the transition from legacy systems to cloud systems."[xliv]

Procurement

Building on the challenges caused by the sheer complexity of managing a large-scale project, governments are also experiencing challenges in scaling government-wide procurement processes due the length of time needed to evaluate cloud-service vendors, which be compliant with government standards before they can be used. Cloud computing services possess certain characteristics that require special consideration during the procurement process.[xlv] This challenge is further complicated by the fact that, at this early stage, many technical standards for cloud computing are unsettled in the industry between vendors. It should come as no surprise that without a leading set of preferred standards in the industry, many governments are still developing their own guidance as to which standards are best for government use.

The public and hybrid cloud deployment models involve hardware infrastructure that is centrally controlled, managed by third-party companies, and, depending upon the circumstances, shared between multiple cloud "tenants" – meaning that customers of the cloud service sometimes share processing and storage resources, separated only by virtual walls. The cloud service providers' employees may also have access to the data or the physical infrastructure being used by the government. This raises some difficult questions about how trust, control, and security should be evaluated in the procurement process. In these models, governments may seek to audit the company's practices to ensure compliance with established security standards, particularly if sensitive government information is being stored or processed. To give an idea of how complicated this can be, consider the US General Services Administration (GSA), which was

transitioning legacy email services to a cloud-based service offered by Google. The US GAO reported that "the process to certify Google to meet government standards for their migration to cloud-based email was a challenge . . . and, contrary to traditional computing solutions, agencies must certify an entire cloud vendor's infrastructure." Ultimately, it took the GSA "more than a year to certify more than 200 Google employees and the entire organization's infrastructure (including hundreds of thousands of services)."[xlvi]

Early in the G-Cloud program, the UK government experienced similar challenges through during early pilots of its "CloudStore" and other public procurement initiatives, which were meant to serve as a streamlined virtual storefront where government CIOs and IT staff could easily compare and acquire new cloud services. When the CloudStore first launched, ambiguities in the procurement framework devised by the government caused confusion over which contract terms governed the relationships between the government organizations – the vendor's standard service terms or the mandatory terms set by the UK government's cloud framework.[xlvii] In part, the framework did not take into account the complex layering and temporal dynamics of contractual agreements between service providers and users. Some scholars have noted that these questions raise some important practical considerations that affect issues related to liability, fairness in the procurement bidding process, and what standards are in fact being met by vendors.[xlviii] Over the last several years, the government has implemented substantial changes in its procurement framework to address these problems.[xlix]

In response to procurement concerns, many governments are now developing or refining unified processes for acquiring new IT services, so government organizations can easily evaluate service options from multiple providers that are pre-approved to meet compliance standards under a standard contractual framework. The US government has since put in place a program – called the Federal Risk Management Program (FedRAMP)[l] – whereby vendors can be pre-certified for widespread use by government agencies. The program envisions the elimination of what would otherwise be a lengthy, *ad hoc* process of certification conducted on a piecemeal basis by individual agencies. A centralized approval process, however, does not necessarily mean a more agile process for approving new vendors, at least during the early periods of such programs. The first FedRAMP authorization was issued in December 2012, nearly nineteen months after the program was launched.[li] As of June 2013, FedRAMP has only approved five vendors – Autonomic Resources, CGI Federal, HP, Lockheed Martin, and Amazon Web Services.[lii] The UK government has experienced similar bottlenecks in dealing with hundreds of vendors seeking approval and accreditation.[liii]

Cultural and Experiential Barriers in Organizations

In some instances, the migration to cloud computing services has been met with skepticism from internal employees. Although this resistance is difficult to quantify, it is often described anecdotally as "cultural resistance." In the case of the US, the GAO has stated that "agency culture may act as an obstacle to implementing cloud solutions," citing an example in which a Department of State employee pointed to public leaks of sensitive information being responsible for putting the agency on a "more risk-averse footing, which makes it more reluctant to migrate to a cloud solution."[liv] While this statement suggests that security risks are the prime concern, others suggest that the negative perception may be more generalized. Martha Dorris, the Deputy

Associate Administrator for the GSA's office of Citizen Services, described her agency's ongoing shift to cloud computing as difficult and cultural, noting that the GSA's "technology team did not want give up the servers" and that a lot of time is spent "moving people along."[lv] The UK government has also acknowledged that difficulties in shifting the culture "will require a significant change in the way people work across the ICT function of government" which, if not addressed, "will impede successful uptake of the G-Cloud principles and approach."[lvi] The private sector experiences many of these challenges as well.

The US has perhaps undertaken the most concerted effort at solving the adoption barrier problem with its "cloud-first" policy.[lvii] Early in its IT reform efforts, the US CIO announced that all executive branch agencies would be subject to this policy, which first required them to migrate at least three IT services to the cloud within an eighteen month period. In addition, agencies are required to evaluate cloud computing solutions before it can acquire off-the-shelf legacy software products. This approach is intended to work as a forcing function to push US agencies toward increased adoption of cloud computing. Although the government has encountered issues, as we have noted elsewhere in this section, the policy initially appears to have had an overall positive effect.[lviii] The cloud-first policy also seems to have influenced other governments as well. The UK government has incorporated a cloud-first policy into its own strategy for IT reform, modeled after the US government's approach.[lix]

Beyond the culture of "buying into" the cloud computing trends, governments are also challenged by their lack of technical experience with the technology. Cloud computing technologies are relatively new to many IT professionals, and there seems to be a learning curve for government IT employees tasked with overseeing cloud services. US agency officials have noted that "delivering cloud services without a direct knowledge of the technologies has been difficult."[lx] Cloud computing involves an "entirely new set of tools and processes," which must be taught to government IT staff.[lxi] As we will explore in the other roles, governments are looking to their technical support organizations and advisory committees, such as the US National Institute for Standards and Technology (NIST), the EU's European Network and Information Security Agency (ENISA), and the UK's Communications-Electronics Security Group (CESG) to develop internal guidelines and best practices regarding government cloud deployments.

Interoperability Between Services and Service Providers

Concerns about the degree to which cloud computing services are technically and legally interoperable are a recurring theme in many government adoption strategies. For any number of reasons – e.g., costs, functionality, or needs – a government organization may wish to terminate relationships with existing cloud computing vendors in order to move to a competitor. Certain factors, like restrictive contractual terms or closed data formats, can make this technically difficult or prohibitively expensive, and in some cases even legally impossible.[lxii] Cloud computing service providers have an interest in making their services as "sticky" as possible to minimize loss of customers to competitors. Ultimately, for the government, this can have the effect of "locking in" IT assets to a particular cloud service provider. These concerns have also been echoed by companies in the private sector looking to use cloud services.[lxiii] On the other hand, some private-sector stakeholder have stated during interviews that an overly standardized

environment could inhibit innovation, and a balance must be struck between these competing objectives.

Conducting extensive due diligence before engaging a service provider and having common standards for interfacing between different services seem to be the prophylactic prescription to the lock in problem, according to the US, UK, and European Commission technical advisors and strategy documents.[lxiv] However, many problems may still remain.[lxv] As described by a US agency official, "it is challenging to separate from a vendor, in part due to a lack of visibility into the vendor's infrastructure and data."[lxvi] Moreover, as the industry continues to emerge, the lack of government standards and best practices may complicate the effectiveness of these approaches.

2. Government as a Regulator

2.1 Overview and Examples

The second prominent role governments play vis-à-vis cloud technology is the role of a *regulator*. Here, the government interacts with cloud computing as it seeks to regulate the behavior of individuals, companies, and others through policy and the rule of law. Across the countries we have surveyed, interventions by legislators, regulatory bodies, or the judiciary are typically *issues-driven* and, in contrast to some of the approaches taken when serving different roles described in this paper, do not follow a "strategy" or "blueprint" of sorts.

Public policy concerns that are debated in national policy circles and global multi-stakeholder forums cover a broad set of issues, ranging from privacy and security to competition law and interoperability concerns.[lxvii] From a bird's-eye view, the diverse issues can be clustered into *two categories*: vertical and horizontal issues. The following list highlights some of the frequently discussed issues in each rubric (but is by no means comprehensive).

Vertical Issues

Issue	Description
Data protection	Data protection arguably ranks top among the concerns related to the cloud. The architecture of cloud computing and the sensitive nature of the data stored in such environments lead to concerns regarding individual rights and related safeguards, such as data quality, processing transparency, and international data transfers.
Data Security	Closely linked to privacy issues are concerns regarding data security, standards, contractual rules, and legal obligations. This category includes, for example, digital signature legislation, breach notification laws, laws regulating how data can be stored in the cloud, but also security audit requirements.
Data retention	Economic regulation as well as national security obligations increasingly require the development, implementation, and operation of retention practices which have to be balanced against civil liberties and other fundamental rights.
Consumer protection	Concerns about the protection of consumers as users of cloud services include the terms and conditions that apply to such uses, the communication between cloud providers and consumers, and the feasibility of consumer protection law to regulate these relationships that are characterized by information and power asymmetries.
Intellectual Property	IP often plays an important role in cloud-based business models, ranging from social media to the publication industry. The exploitation of such rights in the cloud environment is in many cases contested. In particular, the low entry barriers for

	large-scale distribution of copyright protected content causes concerns around piracy on the side of rightholders. IP enforcement mechanisms are also frequently mentioned in cloud policy debates.
Competition	Given the centralized nature of cloud computing infrastructures, questions of ownership, antitrust, and interoperability have emerged. Issues include contractual concerns (e.g., *ad hesion* forms of contracts), the lack of portability, and the conflicts between open and closed standards.
Trade	Restrictive policies – such as the requirement that cloud companies have to register in a given country before they can provide services – that create trade barriers for cloud providers as well as the harmonization of government procurement rules are debated internationally, for instance in the context of multinational agreements such as the Trans-Pacific Partnership (TPP) agreement, or bilateral trade agreements such as the US-South Korea Trade Agreement.

Horizontal Issues

Issue	Description
Jurisdiction, applicable law, enforcement	In order to harness economies of scale, cloud computing often involves the flow of data across jurisdictional boundaries – whether at the local, national, or regional level. From a legal perspective, the global flow of data immediately triggers the questions of jurisdiction, applicable law, and enforcement that are characteristic for Cyberlaw more broadly.[lxviii] In addition, it also raises questions regarding the extent to which global regulation of cross-jurisdictional data flows would be appropriate. For instance, the negotiation of the Trans-Pacific Partnership (TPP) agreement us relevant in this context.
Compliance	Cloud computing providers need not only to obey to general laws, but also to comply with quickly expanding and often very detailed sector-specific laws (e.g., regarding financial, educational, or health data) and master the interplay among them, especially where such laws and regulations vary across jurisdictions.
Transparency	Transparency and clarity are central cross-sectional concerns identified both regarding contractual arrangements as well as regulatory approaches to cloud computing as a technologically, organizationally, and economically complex phenomenon.
Responsibility and liability, incl. cybercrime	Closely linked to transparency and an inherent element for providing an appropriate legal and regulatory framework for cloud computing is the clarification of areas of responsibility for all parties involved. Potential legal frameworks range from traditional approaches (e.g., using criminal law, civil liability, and risk insurance) to concepts such as corporate social responsibility.
Infrastructure	Especially in emerging economics, but to a certain extent also in countries with advanced cloud strategies such as the US and the EU, the availability and competitiveness of infrastructure that supports the digital economy and cloud computing has been identified as an important policy topic, as the often controversial discussions around national broadband plans illustrate.

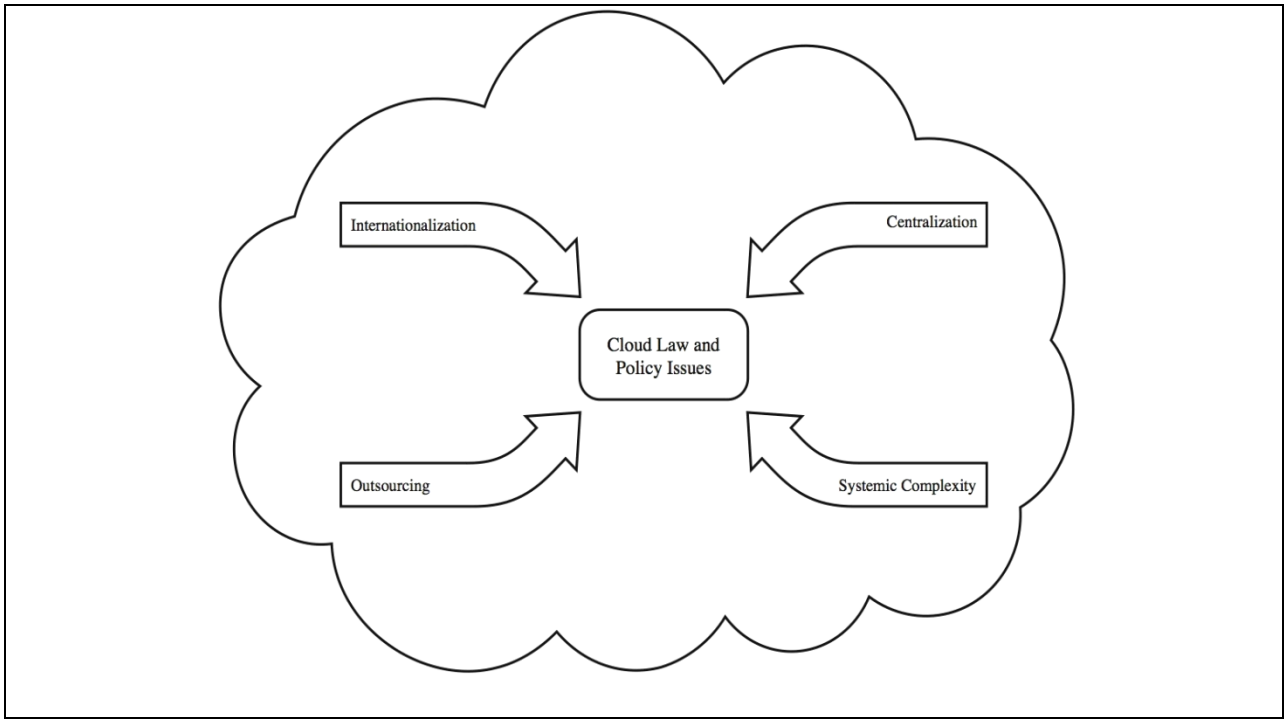
In reality, vertical and horizontal issues often *interact* with each other. A case on point is the interplay between the privacy and transparency debate in the EU. The European Data Protection Supervisor (EDPS) has raised concerns about the privacy implications of consumer use of cloud services. Many EU opinions have highlighted the lack of transparency in contracts about responsibilities and practices.[lxix] The EDPS notes in particular that "the contract asymmetry between service providers and clients" could "lead to an undesirable allocation of responsibility in relation to compliance with data protection law."[lxx] Consumers may be exposed "to a considerable increase of transfer in personal data over networks, involving many different parties and crossing borders between countries, including outside the EU."[lxxi] Also of great concern to

the EDPS is ensuring that cloud computing service providers do not escape the application of the data protection regulations in the EU, due to ambiguities in the wording of regulation text – for example, whether in certain instances cloud service providers would be considered a "processor" rather than a "data controller."[lxxii]

2.2 Analysis and Discussion

(a) Rationale for Regulation

The legal and policy issues related to cloud computing mentioned above read in many ways like the long list of challenges that have emerged in the context of information and communication technologies more broadly. This begs the question as to what extent the cloud environment raises questions distinct from those raised in the context of cyberlaw issues more generally. While there are arguably only a few issues that are truly "new," we suggest that four characteristics of cloud computing – one might call them "*risk vectors*" – at least significantly shape the *risk assessment* of cloud computing from a legal and policy perspective.



The four risk vectors – many of which share commonalities with the risks we noted in the Government as a User section – can be briefly described as follows:

1. *Outsourcing:* As one scholar puts it, cloud computing "can be defined as the ultimate expression of outsourcing,"[lxxiii] where a customer contracts out computing resources and, depending on the specific model, also business data that is processed and stored by the

cloud service provider. Legal risks include performance related problems, security risks, and multi-faceted privacy concerns related to "big data."

2. *Centralization:* In order to benefit from economies of scale, cloud computing depends on relatively centralized architectures, especially at the infrastructure and platform levels. As a result, a small number of very large companies provide the lion's share of cloud products and services. The high degree of centralization of "computing power" gives reason to a variety of concerns, ranging from security vulnerability ("central point of failure") to competition issues.
3. *Internationalization:* In cloud computing environments, data typically flows across jurisdictions and is allocated dynamically depending on the available processing resources, which enables efficiency gains and cost savings. While location-based fragmentation of data storage and processing is possible and practiced, it is arguably in tension with the promise of cloud computing. Either way, the cross-border flow of data shapes legal and regulatory risk assessment across a number of dimensions, including national security, consumer protection, and enforcement issues.
4. *Systemic Complexity:* Cloud computing is built upon and embedded in a complex, layered ecosystem where the moving parts and layers not easily visible from any one perspective. Cloud technology is challenging to understand for non-experts, especially at the level of infrastructure and platform. At the same time, even relatively straightforward cloud services require the working together of various providers, whose contractual relationships are not obvious to the user. These features – several more could be added – contribute to the existing and perceived complexity of the phenomenon, with ramifications for law and policymaking.

(b) Modes and Instruments of Regulation

The various debates concerning cloud computing issues focus not only on risk identification and assessment as we move from a highly decentralized to a more centralized computing environment. That is, identifying an issue to be regulated and a supporting rationale. Legislators and regulators must also consider the appropriate *modes* of regulation when dealing with risks and challenges.

At a basic level, response strategies include: (a) top-down approaches where governments directly seek to intervene into the cloud computing environment, or alternative and sometimes use more "collaborative" approaches, including (b) processes of co-regulation or (c) industry self-regulation. Examples for each category include the following:

a. *Direct intervention*: Lawmakers intervene through the familiar top-down legislative processes by creating a law to address an issue. Examples specific to cloud computing include the proposed updates to the US Electronic Communication Privacy Act (ECPA)[lxxiv] and the recently proposed privacy regulations in the EU, such as the General Data Protection Regulation, are drafted with cloud service providers in mind.[lxxv]
b. *Co-regulation*: In this mode of regulation, the government sets the ground rules for private actors – in this case typically cloud computing providers, who are granted a high degrees of flexibility as to the process of how to achieve the goals the government sets out. Some of the NIST-facilitated standard-setting initiatives in the US fall into this

category, where industry players, governments, and other constituencies work closely together to address a regulatory issue.

c. *Self-regulation*: In this mode, private industry rather than the government is primarily responsible for determining and policing acceptable industry practices. Self-regulation can be independent of or parallel to governmental regulation. The EU has proposed that the industry establish model contract terms and practices as means of self-regulation.[lxxvi]

Governments typically consider the different modes of regulation on an *issue-by-issue basis* – as opposed to a general decision regarding the contours of a cloud computing governance regime. For instance, the European Commission seems to prefer direct interventions concerning privacy challenges while considering co-regulation or self-regulatory initiatives with regard to contractual issues, such as standard terms or the setting of specific standards.

Against this backdrop, *blended approaches* to cloud regulation have emerged across jurisdictions, which contribute to the complexity of the global legal and regulatory framework governing the cloud computing ecosystem. In some jurisdictions, however, direct interventions seem to be the dominant approach. The legal culture and framework of the respective country shape the default mode of regulation.

Importantly, not all of the interventions are aimed at introducing additional *constraints* on the market forces that drive the cloud technology environment. To the contrary, some of the legal and policy measures serve an *enabling* (e.g., cross-border transactions) or *leveling* (e.g., reduction asymmetries in contracts) function.[lxxvii]

(c) Response Patterns

Similar to patterns identified in Internet law and policy more broadly,[lxxviii] legal systems across the countries we studied have responded in one of two ways when confronted with emerging cloud computing issues:

The first response pattern is often the default response to technological change, as it is the easiest for policymakers and produces the quickest results. When a new technology arises, the legal system and its actors seek to *apply existing laws* to the arguably new problems triggered by it (a process often described as "subsumption"). This has already started to occur with cloud computing. For instance, courts in several countries we surveyed have applied copyright law to disputes involving cloud computing services and service providers. In 2007 and 2008 a series of cases involving copyright disputes over a new cloud-based digital video recorder (DVR) technology for television that enabled users to record and playback video from servers located on company premises. Specifically at issue in the case was the manner and location in which the technology recorded and replayed videos, and whether Cablevision, the marketer of the product, could be held liable for copyright infringement carried out by its users. Although the characteristics of the technology were somewhat unique, the Court of Appeals for the Second Circuit ruled in favor of Cablevision, interpreting existing precedent to apply readily to the facts of the case.[lxxix] A Japanese court dealt with a similar issue in the MYUTA case, which involved a cloud-based music storage service that allowed users to upload, access, and playback music from remote servers via mobile phones. In this case, however, the Tokyo District Court ruled in

favor of the plaintiff after analyzing the issues in light of existing legal precedent.[lxxx] As an aside, copyright disputes such as these often serve as an early warning system for potentially unwelcome technology shifts in the ICT ecosystem.[lxxxi]

The second response pattern, which is typically slower than interpreting existing laws, is when the legal system responds to a new technology by *creating new law*, either court-induced or by interventions on the part of the legislature through introducing new legislation that amends existing law or introduces new law. In Europe, the proposed rules on data portability of the data protection framework can at least in part interpreted as a response to cloud computing. The European Commission has also identified a series of issues that might require legislative action in its cloud strategy paper, including a regulation on a common European sales law in order to foster cross-jurisdictional transactions. Policymakers in the US have proposed revisions to Electronic Communication Privacy Act (ECPA), which is often the target of criticism for its nearly 30-year-old provisions regarding wiretap laws, is another example of a regulatory response to cloud computing technologies.

(d) Regulatory Tools and Instruments

Governments have a broad range of instruments available to pursue particular regulatory objectives. This includes traditional regulatory instruments such as command-and-control, incentive-based regulation, and market-harnessing controls, among others. In the cloud computing context, the use of the respective instruments is closely linked to the role the government seeks to play and, connected with it, the rationale for and modes of regulation as outlined in the previous paragraphs.

The following few examples – several more could be added –give a sense of the *variety of available instruments*, which apply specifically or generally to cloud computing providers:

Instrument	Description	Example
Command and control	Direct interventions to exercise control by imposing rules or standards backed-up by sanctions	Revision of privacy legislation to ensure privacy safeguards for cloud environment (EU; US);[lxxxii] Registration requirements for Cloud providers.
Incentive-based	Influence behavior by imposing negative or positive taxes, deploying grants or subsidies, etc. from the government	Use of procurement power to stimulate growth of cloud ecosystem by supporting SMEs (UK)[lxxxiii]
Market-harnessing	Regulatory interventions to sustain certain levels of competition that benefits users and the public	Competition law and antitrust investigations triggered by the market share and/or certain practices of cloud service providers (US; EU)[lxxxiv]
Disclosure	Interventions aimed at structuring the disclosure of information to provide consumers with sufficient data on products and services	Data breach notification laws (US; EU)[lxxxv]
Rights and liability	Allocate rights and liability to encourage socially desirable behavior	Sector specific liability laws applicable to cloud solutions, e.g. health or financial markets (US, UK) Proposed Cloud Computing Act of 2012 (US)[lxxxvi];

It is too early to identify *trends across jurisdictions* and lessons learned with respect to the use of these and related instruments. However, our initial country case studies suggest that command-and-control, disclosure, and rights and liability schemes currently play a more prominent role than others. Based on experiences in other areas of technology law and policymaking, we expect the full repertoire of instruments – including, for instance, insurance schemes – to apply to cloud computing issues more comprehensively over time.

3. Government as a Coordinator

3.1 Overview and Examples

Governments often act as *coordinators* of the evolving cloud computing environment. As a nascent sector, the cloud computing industry is still developing common technical standards, protocols, and guidelines that enable private and public service providers to offer highly interoperable products and services that better serve the needs of users. Governments are playing a powerful role in convening stakeholders, developing collaborative solutions, and pursuing consensus between companies, governmental agencies, international organizations, and other actors in the cloud computing industry. We see the government taking action across three interrelated areas: (a) standard setting, (b) information sharing, and (c) consortium building.

(a) Standard Setting

A prime example of the important role that a government unit can play in cloud standard setting initiatives is the National Institute for Standards and Technology (NIST) in the US. It has taken on a central role in defining standards and collaborating with agency CIOs, private sector experts, and international bodies to "identify, prioritize, and reach consensus on standardization priorities" around cloud computing on both the domestic and international levels.[lxxxvii] By far, NIST is one of the most active organizations across all governments working in the standard setting space. For example, one ongoing NIST initiative – called the Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) – is focused on collecting and generating cloud system specifications and demonstrating how such specifications can be implemented in practice.[lxxxviii] NIST is working closely with private-sector companies and technical stakeholders via its standards roadmap program to identify gaps in standards.[lxxxix] In other initiatives, NIST is assisting the US government's adoption of cloud computing services by developing cloud security standards and a systematic process for certifying cloud providers to expedite the government's procurement of cloud systems.[xc]

The importance of standards has also been identified as one of the key priorities in Europe.[xci] What differentiates the European Commission's initiative from the approaches being implemented in other countries, though, is that it is aimed at "enabling and facilitating faster adoption of cloud computing throughout all sectors of [Europe's] economy" rather than for primary use by just the public sector. The European Commission notes that "vendors have an incentive to fight for dominance by locking in their customers, inhibiting standardized, industry-wide approaches."[xcii] Although the European Commission recognizes that many private

standards development organizations are already at work on cloud standards in Europe, the European Commission believes that additional standard setting initiatives will be needed to ensure that systems are sufficiently interoperable, secure, compliant, and safe for the environment.[xciii] To this end, the European Commission has tasked the European Telecommunication Standards Institute (ETSI) and the European Network and Information Security Agency (ENISA) to collaboratively develop with industry stakeholders a map of the necessary standards and voluntary certification schemes by 2014.[xciv]

Some standard setting efforts are increasingly being organized across between national and international standards development organizations. NIST and ETSI, for instance, jointly held a conference and subsequently set up an ETSI Cloud group to consider cloud standardization needs. ETSI has contributed to the NIST roadmap for cloud standards. The European Commission believes that cloud "will be an important working area in the next year's ETSI work programme."[xcv] ETSI is also actively reaching out to other organizations of interest, including the International Telecommunications Union, International Organization for Standardization (ISO), and Japan's Global Inter-Cloud Technology Forum (GICTF).[xcvi]

(b) Information Sharing

Many governments are providing forums and other collaborative mediums for private sector cloud computing companies, industry experts, standards development organizations, and government representatives to share information and form strategic alliances. The European Commission's cloud strategy, for instance, brought about the creation of the European Cloud Partnership (ECP), which is intended to bring together industry consortia with public officials to support the development of a harmonized "single market" for cloud computing across Europe.[xcvii] It seeks to address the fragmentation of public sector market and to drive the first steps towards better public procurement of cloud services in Europe.[xcviii] The ECP will also support the European Commission's work on standards and certification schemes and help identifying cross-border and interoperable cloud pilot projects "in mission-critical areas of business and public life".[xcix]

In addition, the Standards and Interoperability for eInfrastructure Implementation Initiative (SIENA) perhaps reflects a more targeted initiative funded by the European Commission's Framework Programmes for Research and Technological Development. SIENA's objective is to "accelerate and coordinate the adoption and evolution of interoperable [distributed computing infrastructures] through engagement with [standards development organizations] and other major stakeholders."[c] As a Coordination and Support Action organization, a particular type of organization under the Framework Programmes, SIENA's purpose is to build bridges among standard setting organizations and facilitate the creation of roadmaps that emphasize interoperable standards for cloud computing in research applications.[ci]

(c) Consortium Building

An interesting country case study of government's involvement in consortium building is Japan, where the National Institute of Information and Communications Technology (NICT) together with the National Statistics Center (NSTAC) and the Ministry of Internal Affairs and

Communication have established the "Cloud Testbed Consortium." This consortium convenes communities and working groups from the private sector in order to share information as well as discuss financing opportunities, and collaboratively work towards solutions for the NICT government database.[cii]

3.2 Analysis and Discussion

(a) Importance of Coordination and Standard-Setting

Though often overshadowed by more headline-grabbing issues, such as privacy and security, technical standards play an exceedingly important role in the ICT industry. At a very basic level, a standard can be a common practice, convention, structure, format, or other criteria that defines technical characteristics at the physical, data, application, or network layers in a system. Without diving too deeply into the complex standard regimes, it is worth noting that not all standards are created equal. There are numerous pitfalls and tradeoffs, which can affect factors such as the technical capabilities of and interoperability between systems and competition within the industry. The company or consortium with the leading standard can often profit financially from or exert control over how a standard is used. Standards are created in a variety of forums, through formal and informal "top down" and "bottom up" development processes led by private industry groups, consortia, the government, and international organizations.[ciii]

The lack of cloud computing standards is fueled by the fact that the industry's products and services have not yet matured, and the growing landscape of industry players is still in flux. Reports have indicated the lack of standards is a barrier to widespread adoption in both the public and private sectors. This may have an impact on the market uptake for cloud services in the public sector and in the public sector, as well.[civ] On the other hand, some stakeholders suggest that too many standards can stifle innovation.

Governmental interest in seeing a well-developed body of standards is multifaceted. A well-developed body of standards often reflects a sophisticated and advanced market, which would encourage robustness in the industry domestically and internationally and positively impact commerce. Standards are also useful for governments, especially as they increasingly become users of cloud computing services. Open standards, in particular, also facilitate the sharing information between competitors and serve as a level-setting mechanism, which can help feed downstream innovation and advance the industry as a whole. This may explain why all the governments we surveyed are also interested in both strengthening and influencing the standards development process. In contrast, governments in some of the less developed cloud environments have not fully engaged in standard setting initiatives.

(b) Challenges

Particularly in the case of an emerging industry such as cloud computing, government intervention in the standard setting processes can have substantial drawbacks. Historically speaking, government-led standards can still fail to achieve universal or widespread adoption in the industry. As one scholar describes it, "the risk of getting it wrong is very high and the consequences may be very large because technology that has broad economic and social impact

advances rapidly."[cv] This risk seems to be accentuated when the industry at issue is relatively new and volatile.

The private sector generally has far greater expertise and knowledge than the government when it comes to standards development. In this sense, private-sector-led processes may be more effective than government-led processes. Determining the right mixture and degree of government intervention is therefore critical to a positive outcome. This may be why we are seeing the governments assuming more collaborative and supportive roles as a coordinator in the cloud computing standards processes, rather than by taking a more proactive approach and creating mandatory standards.

On the other hand, if a government were too passive, there is also a risk that the private-sector led processes could themselves fail to produce the necessary standards, leading to negative side effects in the marketplace. For example, this potential outcome has concerned the EU in the context of interoperability. As stated in its cloud computing strategy, "despite numerous attempts to develop standards for clouds, mostly led by suppliers, there is a strong risk that clouds will lack interoperability and data portability (withdrawal of data)."[cvi] At the same time, processes that are led purely by private industry may lack the incentives for private stakeholders to commit to interoperability and data portability at this early stage.

Finally, while much opportunity exists for governments to influence domestic standards, many forces are driving companies towards globally-harmonized standards. This is reflected by a growing number of provisions within international trade agreements as well as influenced by international organizations like the World Trade Organization (WTO) and the International Telecommunications Union (ITU). Some countries, such as the US, have already established a firm foothold in the global cloud computing marketplace, and it seems reasonable to think that these companies may be able to leverage their market positions to influence the international debates.

4. Government as a Promoter

4.1 Overview and Examples

Across the activities described before, governments have become *promoters* of cloud computing technologies. More specifically, governments seek to encourage the growth of the private cloud computing industry and its technologies using a set of targeted policy tools that stimulate economic growth and industry-sector innovation, support emergent startups, raise awareness and mark approval of new technologies, foster competitive markets, and encourage the adoption and use of cloud computing technologies.

The reasons why governments are promoting cloud computing are varied. As noted earlier, cloud computing offers an enormous potential for economic growth and the possibility of reshaping the IT industry landscape. If these benefits are fully realized, the economic futures of the IT industry within a given country may be closely tied to the health of the resident cloud computing companies. The emerging cloud computing industry may also have a substantial and

continuing impact on a country's overall economic performance. Beyond competitive advantage and economics, governments may also desire strong cloud computing industries for purposes of strengthening national security of the Internet infrastructure in the private sector. With these points in mind, it should come as no surprise that governments are actively promoting the cloud computing industries within their borders.

(a) Promotion by Adoption

As noted above in the "Government as a User" section, many governments are implementing large- and small-scale efforts to shift IT resources from legacy system to cloud-based systems. These programs are funneling large amounts of revenue into cloud companies, and supporting the emerging industry; governments are quickly becoming the cloud industry's largest customers. The benefits to the market are many. Government contracts awards are often very lucrative arrangements for the private sector that also strengthen the marketplace for products and services, and, occasionally, spark further innovative developments. Historically, a number of technology companies have been able to transform products and services originally created under a government contract into widely successful commercial products.[cvii]

(b) Promotion by Endorsement

By adopting cloud solutions, a government at least implicitly signals its support for the technology and often gives the cloud computing industry visibility. Sometimes this endorsement manifests as an explicit statement, in a policy announcement or comment to the media, while in other cases the endorsement remains implied when a government elects to adopt cloud services over other options.

A prominent example in the category of public endorsement is the US. When its "Cloud First" policy was introduced in February 2011, the announcement caught the attention of news media and received mixed reactions.[cviii] The *New York Times* noted concerns from government employees and questioned whether cloud computing is a feasible solution for the government given recent high-profile outages at major cloud computing providers and the government's track record of investing in expensive projects that fail to produce results.[cix] Meanwhile, others lauded the government's move to newer, cost-reducing technologies.[cx] Still, the US government's policy announcement was both an endorsement for and a showcasing of the economic benefits of cloud computing, complete with detailed data forecasts of how the implementation is beneficial to the government. Similarly, in October 2011, when the UK government launched its "G-Cloud," it emphasized in public statements how cloud computing will "transform the Government ICT estate into one that is agile, cost effective, and sustainable."[cxi] While statements are often intended to highlight the government's rationale in making decisions, they also function strongly as a public nod of approval.

Governments have found other ways to showcase how they are using cloud industry services. For example, the US General Services Administration (GSA) launched an online cloud services storefront at http://info.apps.gov to help governmental agencies to compare cloud services prior to making a procurement acquisition.[cxii] More than fifteen case studies of US agencies are available on this website, each of which explains in some detail how the agency has implemented

and benefitted from cloud computing in some manner.[cxiii] The Info.Apps.Gov website is intended to serve other functions as well. A critical component of the US IT reform plan is that individual agencies, each of which make IT procurement decisions independently, must actually make the decision to procure a cloud service. To this end, Info.Apps.Gov is also a tool to help US government agencies manage the procurement process and compare services from cloud vendors.[cxiv] A more comprehensive program aimed at streamlining US government procurement, known as FedRAMP, is also underway. This initiative promises to develop a uniform framework for federal agencies to assess and acquire cloud services.

As noted in the Government as a User section, the UK government is also using an online cloud services store, which they call the "G-Cloud AppStore." Similar to the US government's apps.gov, the G-Cloud AppStore is a tool that enables governmental agencies to compare service offerings prior to procurement. Beyond this basic function, the UK government intends for this storefront to become an "open, visible, commoditized and cost-transparent marketplace, where all relevant public-sector IT services can be found." The government hopes that this will increase the performance of cloud services by serving as an open feedback mechanism. A core component of the UK G-Cloud strategy is specifically aimed at small-to-medium sized cloud businesses, as part of a concerted effort to stimulate new market entrants in the industry.

Although it is difficult to measure the impact of government endorsement of the cloud industry, it is indisputable that the government's ability to endorse particular technologies and industries is a tool that can be used to influence the public's perception of cloud computing and the rate at which its products and services are adopted by public sector entities.

(c) Promotion by Funding and Incubation

Beyond acquiring services and marketing, governments are increasingly offering funding to existing companies and industries and finding new ways to incubate technology innovation in the cloud industry. They may financially support applied or basic research, venture funding, and enable open access to government hardware, software, and data resources. France, for example, has recently announced that it would fund two cloud companies directly.[cxv] These startups are also funded by other private investors, and operate with the promise that they will create data centers in France that will keep the data and software of its customers secure. In the UK, the government has set aside £40M in its "Notion Capital" fund," which will reportedly be used to support pan-European cloud small-to-medium-sized enterprises (SMEs).[cxvi] In this instance, public funding is being used to promote smaller cloud companies and new market entrants, rather than the larger established tech companies – a theme that echoes throughout the UK's cloud strategy plans, which the government hopes will foster a more competitive cloud market in the UK.

Several governments have introduced *innovation incubation centers*, and opened non-production hardware and software environments to developers. The UK government has plans to launch a "cloud skunkworks," which will serve as a government technology incubation hub, where innovative companies develop and create new government ICT solutions in a real-time development environment. This would ideally encourage creativity and incentivize a wide range of potential cloud-service providers, particularly SMEs and other entrepreneurs, to try their hand

at developing innovative services for the UK government without the need for investing in a expensive hardware and software development environment. The Japanese government offers similar development environments through what they call the "Japanese Testbed Consortium." The Testbed also invites cloud service providers to use government hardware and databases to create ICT government solutions.

4.2 Analysis and Discussion

(a) Intervention Points

The various means by which governments promote cloud technology and industry in order to accomplish the objectives mentioned above can be roughly clustered into two main intervention points:

Demand side interventions: On the demand side, governments are playing the role of promoters as they stimulate adoption of cloud-based services by becoming users and marketers. Increasingly, cloud computing has become a central factor in long-term government IT reform policies, and has become the subject of positive mentions in government policy announcements. These actions showcase the industry and implicitly endorse such technologies – akin to "if it's good enough for the government, it's good enough for consumers and companies to adopt as well."

Supply side interventions: In terms of supply-side interventions, governments are funneling large amounts of capital directly into companies through incubation programs, and as they become procurers of cloud services. Governments are also finding ways to stimulate existing and emerging companies by providing hardware and software development environments, and encouraging companies to innovate. More indirectly, governments are supporting industry by developing and making improvements to the core infrastructure upon which cloud companies heavily rely. Interestingly, the use of legislative and regulatory tools to promote the industry and its technologies is not as widespread as one might expect give the calls from private companies and the public for harmonization of security and privacy-related laws across borders.

(b) Emerging Approaches

Outside of these two main intervention points, some countries have taken alternative approaches. Rather than funneling financial support directly to the industry, some countries have found more indirect means of supporting the cloud industry's growth.

One example is the Infocomm Development Authority (IDA) of Singapore's the Cloud Innovation Centre (CIC). The CIC was established to help companies build private clouds and address the new technical challenges presented by cloud computing. It works in partnership with private industry leaders. One especially interesting CIC initiative aims to build a next generation broadband network that is capable of delivering gigabit speeds to all homes, offices, and schools with a complementary wireless component that covers public areas. The CIC hopes that this

initiative will support the development of the cloud industry by removing infrastructure barriers and other networking bottlenecks.

(c) Challenges

As is the case with many of the other roles we have analyzed, a key challenge for the government is that the cloud computing industry is still evolving at a very rapid pace. While the industry promises much economic growth, others fear that it represents the next overhyped "technology bubble."[cxvii] While cloud computing services do present cost savings with economies of scale, they may not be appropriate or beneficial in every instance for small companies.[cxviii] Other critical questions, such as data ownership, interoperability, security and privacy may prove to be impenetrable obstacles to widespread adoption, too. The government may put itself in an awkward position of promoting a technology before it has presented regulatory solutions to these questions.

Because cloud computing is generally speaking a centralized model, the intermediary network pathways will play an increasingly important role in the cloud computing story. While cloud computing companies can develop technical solutions to make their services more reliable and robust, they may not be able to address weaknesses in the Internet backbone or other infrastructure, whose development must occur on a global scale to truly maximize cloud computing benefits. The ongoing network neutrality debate – regarding ownership and control of the Internet and restrictions on use of Internet bandwidth – also presents a unresolved challenge to the cloud computing industry.

5. Government as a Researcher

5.1 Overview and Examples

Cloud computing presents new challenges not only for the companies developing the technology, but also the governments who seeks to use, regulate, and promote these technologies. At the same time, many think the cloud industry is only just being to scratch the surface of its capabilities. In determining the best courses of action regarding their approaches to the cloud, governments seek answers to key questions about the economic and societal effects of cloud computing technologies, and also to help the industry find solutions to technical problems and limitations.

In this role, governments are becoming *researchers* of the cloud by conducting inquiries through their agencies and funding the research of academic institutions, think tanks, and other organizations on these issues. As researchers governments hope to build an extensive technical and policy knowledge base to better understand cloud issues, explore the opportunities and risks that the cloud has to offer, and encourage private-sector research and development. There are two key intervention tools that governments have at their disposal: research conducted by government agencies and government-funded research by private organizations. And, as you might expect, this role overlaps with other roles, including the user, promoter, and coordinator roles.

(a) Research Conducted by Government Organizations

A number of governments currently have *extensive research programs* on cloud computing, which range from studying issues associated with security and interoperability to specific deployment scenarios based on use cases like health care data systems and government procurement. Some of this research is very focused on governmental needs, while other efforts are more broadly scoped.

In the US, NIST has been conducting research on cloud adoption for the last several years. NIST's cloud computing program was born out of the US government's need for a technical aide to complement its ongoing IT reform efforts.[cxix] In the long term, however, NIST's goal is "to provide thought leadership and guidance around the cloud computing paradigm to catalyze its use within industry and government."[cxx] Although much of NIST's outputs are aimed at increasing the government's understanding of issues and its adoption rate, a portion of its website is – titled "useful information for cloud adopters" – is targeted at a wider audience and could be useful for consumers and companies in the private sector.[cxxi]

In the EU, the European agenda for cloud computing includes a list of policy items that the EU believes should be addressed in research and policy to ensure that the cloud industry has accelerated growth and competition across Europe's economy.[cxxii] At the top of this list is "digital fragmentation" – the lack of harmonized legal and regulatory frameworks across EU member states – as well as contractual issues surrounding responsibility for liability, data ownership and portability, reliability, and on the lack of standards to ensure sufficient levels of interoperability. This research track aims to inform policymaking at the EU level, with a particular focus on level-setting the disparate legal structures used across European Economic Area.

(b) Research Conducted by Government-funded Private Organizations

In addition to conducting research through government-run entities, governments are also funding a wide variety of basic and applied research in the private and educational sectors.

The US government has funded a large number of these programs through the National Science Foundation (NSF), an agency which provides billions of dollars of funding for fundamental research in science and engineering fields at education institutions. Since at least 2009, NSF has focused on issues such as security and privacy, trustworthiness of cloud providers, networking in the cloud, algorithms and data management, and software engineering in the cloud – to name but a few.[cxxiii] Some of these research projects are also funded in partnership with private companies who have a stake in the cloud computing industry.[cxxiv]

In *Europe*, research initiatives are being funding both at the EU-level as well as at the member and non-member state level. For example, the European Commission's "Framework Programmes for Research and Technological Development," which are a series of EU-government backed funding initiatives aimed at research across the EU, funnel billions of euros into universities, small-to-medium sized private enterprises, public institutions, international

organizations, and individuals.[cxxv] Currently, the European Commission is soliciting proposals from applicants to be part of the seventh iteration of the Framework Programme – know as FP7 – and is plans to award more than €50 billion over the course of the program, from 2007 to 2013.[cxxvi] So far, the European Commission has invested several hundred million euro into more than fifty cloud computing related projects under FP7.[cxxvii]

Some governments are closely watching the state of the cloud computing industry – and programs like FP7 – for indicators that industry needs are being met. In 2011, the German government's Federal Ministry of Economics and Technology – Bundesministerium für Wirtschaft und Technologie – commissioned studies from private consulting firms, including Booz & Company, to analyze particular aspects of the cloud computing industry in Germany and inform a course of action by the government.[cxxviii] One study, which investigated standards and interoperability, lead the Ministry to recommend that "rapid action is needed since crucial decisions are likely to be seen by 2014, meaning that the future course will have been determine by then."[cxxix]

Similar to developments in Europe, the Japanese government also has a number of ongoing initiatives related to supporting cloud computing research. The "ASP-SaaS-Cloud Consortium," which has also been a useful tool for the Japanese government's promotion and coordination of the cloud computing industry, conducts government-funded research to create guidelines and case studies relating to data security, reliability, public procurement, and management of medical information, among others.[cxxx]

5.2 Analysis and Discussion

(a) Challenges

Based on our review, governments rely heavily on input from industry stakeholders to identify the relevant technical and regulatory issues that should be addressed in government-driven research programs. This makes a lot of sense, as it relates closely to a problem noted in previous sections regarding how private industry has far more expertise and capacity for understanding the key issues in an emerging industry. However, the potential challenge for the government is the influence that private stakeholders might have in shaping the research focal points and driving outputs towards certain objectives and interests.

In turn, this may affect the government's approach to its other roles. Alternatively, the private sector may direct governmental action in the wrong direction. To give a brief example where this seems to have happened already to a small extent in the regulator context, consider NIST's work on defining cloud computing, and effort that was primarily undertaken to aid US agencies in the IT reform efforts. [cxxxi] Not long after NIST published its final definitions, a representative in the US legislature, through the proposed "Cloud Computing Act of 2012" – also noted briefly in the government as a regulator section – that sought to amend existing legislation to incorporate identical definitions of cloud computing into a US criminal statute that prohibits unauthorized access to computer systems.[cxxxii] The proposed bill was attacked by legal scholars for its definitional imprecision, who noted "this definition of cloud computing service probably

becomes co-extensive with the Internet generally" and that the bill sounded "more like a vendor's sales pitch than a basis for criminal prosecutions."[cxxxiii]

Another challenge that the Cloud Computing Act of 2012 proposal hints at is balancing government-driven research aimed at advancing technology with exploratory research aimed at identifying more relevant legislative gaps or opportunities for policymakers. With some notable exceptions, we observed during our review that many research efforts seem to be primarily focused on advancement of technology or standards development. The EU, in contrast, specifically identifies such research in its strategy plan as a priority alongside research aimed at more technical development. That said, it is quite possible that many countries may have ongoing research on such topics through their legislative bodies that is publicized.

6. Government as a Provider

A small number of sub-government entities, such as individual agencies or departments within a government, have begun to offer cloud computing services to other agencies or to the public. In this *emerging role*, these governmental organizations are assuming the role of a service *provider* to others.

The US Department of Agriculture has reportedly been developing a large private cloud computing infrastructure to support its own IT needs and to offer cloud computing services to other government agencies.[cxxxiv] Although not much is publicly known about the program, it could be an interesting model for other governments to replicate.

China has also become a cloud service provider, but instead of serving other agencies it plans to provide support the private industry. The city of Wuxi in the Jiangsu province is home to a government-funded data center that the local government developed in partnership with IBM. The data center will offer cloud computing services to more than 2,000 software vendors in the nearby region as well as local businesses. Reportedly, IBM is sharing revenues with the local government, and plans to expand this model to other regions in China with the support of the national Chinese government.[cxxxv]

III. Observations and Policy Considerations

1. Introduction

The preceding section described a number of roles and instruments that governments are using to engage cloud computing, and highlighted a series of challenges that governments are facing in each role. Building upon these examples, in this section we share higher-level observations about the roles and governments strategies. These observations are primarily driven by case studies and are anecdotal in nature, as the sample size is too small and the field (technology, markets, etc.) too nascent to make any empirical claims. As such, the list of issues presented below is by no means comprehensive, but hopefully at least illustrative for the types of policy

issues governments around the world need to address when considering the various roles, approaches, and tools outlined before vis-à-vis the evolving cloud ecosystem.

2. Cross-Sectional Observations

2.1 Context Influences Governmental Objectives

Among the bigger picture insights gained from our review is the high degree to which the economic, political, organizational, and cultural *contexts* appear to influence the objectives governments seek to pursue with cloud computing, what roles they are willing to emphasize, and what instruments to deploy. The fact that context matters is not a new insight; context routinely is routinely a factor in policymaking. However, considering that many industry proponents view cloud computing as a "game changing" technology, it might be surprising nonetheless as to what extent existing contextual circumstances shape – this may also mean constrain – a government's cloud vision, strategy, and implementation.

The following examples from the previous section might further illustrate the importance of context:

- Many of the positions the US government has taken across roles – and both domestically and internationally – are at least informed by the economic importance and stature of large US-based cloud providers such as Amazon, Microsoft, Google, and others. Industry insiders, for instance, stated during off the record interviews that the US government's strong and strategic involvement in questions of standard setting is significantly motivated by broader considerations related to the global economy and competitiveness.
- The European Commission's cloud computing strategy – with its emphasis on enabling and facilitating adoption of cloud computing throughout all sectors of the economy and focus on cost savings and job creation is reflective of overall policy goals, the guiding legal framework under which the European Commission operates, as well as Europe's decentralized government structure.
- The strong role of contextual factors in shaping a government's position towards cloud computing was illustrated under dramatic circumstances in Japan, where cloud computing technology was identified as a key resource in disaster and relief management in the aftermath of the devastating 2011 Tōhoku earthquake and tsunami.

Contextual factors not only heavily influence the overall direction and driving goals behind governmental roles, but also shape the approaches taken and instruments used within the respective roles. The way the US and European governments approach to the role of cloud computing regulator follows well-established response patters, and is also deeply embedded in the respective legal frameworks and cultures of these companies.

2.2 Focus on Potential Benefits

Many of the government strategies we reviewed emphasized the *benefits* of cloud computing promises over traditional IT. For example, most governments point to the economic benefits in their rationale for adopting cloud computing for government use and in promoting the technology to the public at large. Other benefits often noted include its innovative capabilities, flexibility, and collaborative capacity. With this in mind, we observed that many strategies appear to lack a thorough discussion of the potential disadvantages of using cloud computing.

While cloud computing is widely acknowledged to impart benefits on its users, empirical evidence of its *actual* benefits in practice is rarely noted in government strategy documentation. Reports have surfaced in private industry that cloud computing may be less useful for certain applications – some private businesses have found that cloud computing services can sometimes be impractical replacements for traditional IT.[cxxxvi] Perhaps even more remarkable than the lack of empirical evidence is that *costs* – including opportunity costs – were also rarely addressed in policy reports and discussions. Admittedly, a cost analysis prove to be a difficult undertaking, as quantifying certain costs, such as those associated with potential technological lock-in effects, privacy, and security, may not be easy. Nevertheless, cost analysis may still be worthwhile, and it is worth noting that governments are increasingly committing to cost-benefit analyses as part of evidence-based policymaking, which arguably yields better results.[cxxxvii]

2.3 The Role of the Private Sector

Across all roles and approaches, the private sector – as in other high-tech areas – plays a key role vis-à-vis the government. In almost all countries we analyzed, companies are the most important providers of cloud computing services, especially in cases where the government is the customer. The biggest exception is arguably China, where the government plays a much more active role in developing and owning the cloud technology infrastructure and where the boundaries between private and public are blurring, given the strong regulation of information and communication technologies under Chinese law.[cxxxviii]

Outsourcing the processing and storage of governmental data to third parties in the private sector has numerous implications. It is clearly important when sensitive government data is at issue – for example, data related to tax collection, law enforcement, and national security. It is also may be relevant for purposes of *government competency*. Governments may wish to maintain more control over their IT assets so that they are not completely reliant on the private sector to keep their systems operational. Moreover, there is something to be said for policymaker competence on technical issues and the extent to which the government looks to the private sector for cues and direction. Governments should expect to interact with technological changes, like cloud computing, on an increasing basis. This requires governments to build and maintain the necessary in-house technical expertise to make sound judgments in the public interest, striking a balance between using their own competence and the expertise of market-driven players.

2.4 Diversified Policy Toolbox

Looking at the interactions between governments and cloud computing, the multitude of postures and forms of engagement a government might pursue becomes quickly apparent. Governments have a variety of tools at their disposal that can be used to direct, influence, shape, or nudge the

cloud computing ecosystem towards reaching policy objectives. The tools we observed in use can be roughly organized into three categories (acknowledging partial overlap and secondary effects).

- *Demand-side tools.* These tools target the users/clients of cloud computing services, including governments, businesses, and consumers to stimulate or otherwise shape the demand for cloud computing services. Examples: "Cloud first" policies; centralized procurement systems; vendor certification programs.
- *Supply-side tools.* These tools target the suppliers and producers of cloud computing services, aiming to stimulate growth or shape the landscape of suppliers. Examples: Government incubation programs; government funded research programs.
- *Level-setting tools*. These tools target discrepancies between the demand-side and the supply-side, and seek to even the playing field and reduce barriers to participation. Examples: Collaborative standards development; open procurement processes.

Governments have a broadest range of tools at their disposal. These tools can be combined with other instruments and across roles to achieve policy objectives. Consider alternative means by which the government may attempt to encourage the creation of interoperable systems. By taking on multiple simultaneous roles, governments may work towards creating a more interoperable cloud ecosystem by exercising its procurement power or facilitating standard setting initiatives, among other activities mentioned in the previous section.[cxxxix]

2.5 Timing Interventions

As in other fast evolving areas of technology, timing is a critical consideration for how and when the government should intervene. In their role as a regulator, for instance, governments need to carefully determine the appropriate time at which to intervene, for instance by adjusting consumer protection or privacy laws, in order to strike the right balance between enabling an environment that facilitates technological innovation on the one hand and providing regulatory safeguards for users and other stakeholders on the other hand.[cxl] Ideally, the government responds to public pressures in making these determinations and engages in a multifactor analysis to determine the right point to intervene with the right intervention. Such an analysis would include an assessment of the maturity of the technology, industry organization, and markets.

Similarly, and looking at governments as users, timing matters when exercising procurement power. Early movers, for instance, tend to have a greater impact on the development of appropriate privacy and security standards when dealing with the private sectors. As soon as certain industry practices and standards are set, they are much harder to influence, as our research on interoperability demonstrates across a number of case studies where procurement was an important tool in the government's toolbox. This arguably also applies to the cloud environment. Taking into consideration the US and UK governments' relatively rocky starts to creating a streamlined procurement systems and hard push hard for government adoption through "cloud first" strategies, they may have achieved better results if they had anticipated the need to establish best practices and government standards before implementing these programs.

In addition to the importance of timing interventions in ways that they can be most effective, it is also critical to recognize that cloud technology, markets, strategies, rationales for adoption and promotion *change over time*. The dynamic nature of the cloud environment requires that governments across roles engage proactively over time with the changing landscape, incorporate a systematic learning process, and adjust their strategies, approaches, and instruments accordingly. In the US, NIST seems to engage regularly with diverse stakeholders through workshops and regularly updates its strategies and guidance documentation over time through an iterative process.[cxli] Although it is still too soon to tell if these initiatives will work as intended, this appears to be an early leading example of how to approach the industry and technology dynamics.

2.6 Different Types of Coordination

Cloud computing as part of the overall digital ecosystem is characterized by a relative high degree of complexity in terms of technology, market dynamics, norms, and regulation. As in other high-tech environment that share some of these characteristics, governments have various approaches available how to deal with complexity, ranging from ad hoc strategies to more holistic approaches. As noted in the previous section, several governments have decided to approach cloud technology strategically, while others remain more issue-driven.

Looking at the subset of countries that have developed cloud strategies, the importance of *coordination* becomes clearly visible. Based on our review, at least three different types of coordination in which governments play an important role can be distinguished:

- *Inter-agency coordination*: When adopting cloud technology as users, governments with cloud strategies have taken coordinated approaches. The US government is a particularly strong example in this respect. As noted in the previous section, the US Chief Information Officer (CIO) and the US CIO Council, consisting of the CIOs from major agencies, coordinated cloud adoption by the federal government. Other governments – for instance in Colombia – also take coordinated approaches, but leave more leeway to the individual agencies.
- *Standard setting initiatives*: The importance of private-public collaboration in the context of cloud standards was already discussed in the earlier parts of this report. Government-facilitated cloud standard initiatives such as the ones under the NIST umbrella in the US, the respective work of ETSI and ENISA in the EU, or NICT and NSTAC in Japan are examples of this second type of coordinative activity.
- *Multi-stakeholder forums*: Beyond standards, government-led coordination is also an important mode of operation when addressing policy issues and developing best practices. Multi-stakeholder processes have gained prominence also in the cloud context. The policy roundtables organized by the Aspen Institute or the cloud report series by the World Economic Forum are illustrative of this third type of coordination.

2.7 Role Conflicts

Perhaps even more than in other areas of ICT, many governments play multiple roles simultaneously in the evolving cloud computing ecosystem. Such a multi-role approach can come with great synergies. For instance, the approach taken by the European Commission to encourage government adoption of the cloud and boost the industry is a situation where the objectives of the government as a user and as a promoter are well aligned. However, as in other domains of society and life, governments might face actual or potential *role conflicts* when exercising roles corresponding to two or more statues.

Based on the map of roles provided in the previous section, one can identify a number of *potential* role conflicts. For instance, conflicts might arise between regulatory compliance (government as regulator) for agencies conflicts with cloud-first strategy (government as user). And there might be tension areas between the roles as regulator and promotional activities for industry. The lack of protective legislation (e.g., security and privacy issues), for example, might discourage private sector adoption both domestically and internationally. Conversely, regulatory burdens – for instance in sensitive areas such as health care of the financial industry – may be greater in the cloud and discourages adoption in the private sector.

A case in point of an *actual* role conflict along these lines are the recent revelations of the US National Security Agency's PRISM plan and its abilities to easily gain access to information being stored at technology companies.[cxlii] Analysts and industry executives expect that the surveillance program by the US government might have substantial negative effects on cloud adoption, both domestically and internationally.[cxliii] Public clouds in particular will be met with increased skepticism, according to these observers, creating an actual conflict between the US government's efforts to promote cloud technology (government as promoter) and its national security programs (government as regulator). Decisions by local data protection authorities in Canada and Europe, which prohibit or discourage domestic or regional government plans to migrate data to the cloud or use US cloud services, are examples of the possible consequences of such conflicts.[cxliv] Already government officials in these countries are discussing these as possible reactions to this program.

While some of these role conflicts might be hard or impossible to avoid, it is interesting to observe that discussion about the potential of any role conflicts has not yet received much public attention in policy circles, not even in countries with advanced cloud strategies such as the US, Europe, or Japan.

3. Policy Considerations

As described in this report, policymakers and other public sector decision-makers are not only in the process of addressing multifaceted issues at the intersection of technology, markets, and law when developing policy approaches to cloud computing. They simultaneously play different roles and, potentially, have to deal with role conflicts at the strategy planning and implementation phases. This level of complexity, paired with the limited availability of solid evidence regarding the effectiveness of different policy choices, makes it difficult to develop

comprehensive "navigation aids" or practical "decision-trees" for the public sector as far as cloud computing strategy development and deployment is concerned.

However, based on the country case studies we have reviewed in the context of this report, at least a series of *policy considerations* for decision makers in the public sector can be distilled and offered by way of *synthesizing* some of the key findings of our exploration:

(1) *Policy objectives*: Our cases studies illustrate that the public sector can develop and implement cloud-relevant strategies, approaches, and instruments for a variety of reasons. Underlying policy goals might include larger objectives such as contributing to a core infrastructure for innovation, growth, and trade, more specific issues such as IT cost savings through efficiency gains. The broad range of objectives and different approaches to pursue them suggest to be as specific regarding as possible regarding the aims when considering policy interventions concerning cloud computing. This includes, as this report suggests, an analysis and assessment of potential policy trade-offs or tensions among objectives.

(2) *Analyze forces at play*: As in other technology-related areas of policymaking, cloud policy-makers need to engage in a multi-factor analysis when considering cloud strategies, approaches, and instruments. Existing legal and policy frameworks, organizational structures (for instance the degree of centralization or decentralization of government), the maturity of technologies and markets (including standards), and related factors – in some cases even geo-political considerations – have to be taken into account both at the design and implementation level of public sector-based cloud strategies. These factors are also likely to create path-dependencies that might limit the spectrum of achievable goals and available instruments.

(3) *Consider mix of roles and instruments*: To pursue cloud-related policy objectives, policymakers and other decision makers can "wear different hats" as our analysis in this report indicates. For each policy goal, policymakers should consider the full range of available approaches and instruments and engage in a comparative cost-benefit-analysis for each option, mapped on a time-line and based on lessons learned from other areas of high-tech policymaking. As our case studies suggest, a blended approach of roles and instruments will often be required to pursue the respective cloud policy objectives.

(4) *Prepare for role conflicts and other complicating factors:* As discussed in the paper, a multi-role and multi-instrument approach can lead to intra and inters role conflicts. Policymakers should anticipate and assess such "interoperability problems" among roles and instruments and plan for ways to limit and/or resolve such conflicts. Another complicating factor identified in the paper is the role of time. Given the technological, economic, and legal/regulatory complexity of the cloud computing ecosystem, cloud strategies need to carefully map and evaluate approaches and instruments on a timeline and synchronize them.

(5) *Build-in mechanisms of learning:* One important (albeit not surprising) take-away from the country case studies is the fact that developing and implementing sound public policies on cloud computing is difficult. The complexity of the technological and market environment, path dependencies and role conflicts, timing issues and the speed of change, or unintended consequences and spillover effects are only a few of the complicating factors identified in this report. Policymakers are well advised to anticipate such

complications when crafting cloud strategies, build-in mechanisms assessment and learning, and even consider "exit ramps" for each approach and instrument.

As the review of various cloud policies by governments in the US, Europe, and selected Asian countries suggest, all the considerations outlined above do not take place in a vacuum, but are embedded in a complicated reality of political and financial economy, cultural factors, among other shifting contexts. These contexts are important and should be taken into account.

IV. Conclusion

The emerging cloud computing industry is catching the attention of policymakers and government CIOs around the world, who are taking on the roles of *users*, *regulators*, *coordinators*, *promoters*, *researchers*, and *providers*. As *users*, governments are adopting public, private, and hybrid cloud deployments for operational use to take advantage of its financial and technical efficiency, innovative features, and ability to facilitate collaborative environments. Governments are also *regulators* of the cloud computing industry, acting through their legislative, judiciary, and regulatory agency branches to develop and implement policy considerations to regulate the behaviors of individuals, companies, and others. In serving as *coordinators*, government may participate actively in the standards development process, facilitate the sharing of information between companies and the government, and encourage the building of consortiums. As *promoters*, governments not only publicly endorse cloud computing technologies as they adopt them as users and call the public to adopt them as well, but also as they directly incubate and fund new and existing companies. In the role of *researchers*, governments seek to understand the technical challenges and societal challenges that technology presents in research initiatives conducted directly by the government or by private entities it funds. Finally, governments are becoming *providers* of cloud computing services by offering services to the public or to other governmental organizations.

Many industry proponents believe cloud computing represents *the next big thing*. It may substantially shift in the economics of technology, enabling new possibilities and new industries, and present opportunities for shifts in technological competencies between countries and international trade. This context shapes governmental approaches to the cloud, perhaps by encouraging governments assume certain roles more actively than others. Some of these roles work well together – for example, the roles of adopters, coordinators, and promoters seem rather synergistic – while others raise difficult challenges and potential ideological conflicts – for instance, in the roles of regulators, users, and promoters the government occasionally sends mixed messages.

There is no silver bullet solution for determining the right mix of interventions, policy tools, and other instruments that governments should employ in their approaches. That said, from reviewing case studies around the world, it seems that policymakers may wish to consider a number of factors when developing their approaches to the cloud. Governments should seek to understand the *policy objectives* and critically *analyze the forces at play* before taking action. As is often the case with emerging technologies, the market structure, maturity of the technology, and other circumstances can change rapidly, prompting shifts in responses. Survey the mix of

roles and instruments available, understand the synergies and tradeoffs between certain roles and tools, and prepare to address *potential conflicts between roles* and other complications. Finally, build in *learning mechanisms* to the strategy to assess whether policy objectives are being met and if course corrections would be helpful or necessary. Many governments have opted to take an iterative approach in their roles to cope with the shifting landscape and technology.

---

[i] "Cloud Computing" is a term that broadly describes an emerging group of related technologies and business models. For purposes of this paper, we generally use this term synonymously with the US National Institute for Standards and Technology's definition, which defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," US National Institute for Standards and Technology, Special Publication 800-145 (September 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Although many of the examples we discuss in this paper involve Software as a Service (SaaS) models of cloud computing, our comments may be extensible to other service models of cloud computing, including Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

[ii] Vivek Kundra, US Chief Information Officer, "Federal Cloud Computing Strategy," US Office of Management and Budget (February 8, 2011), http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[iii] Yasuo Sakamoto, Deputy Director General, Global ICT Strategy Bureau, Ministry of Internal Affairs and Communications (MIC), Japan, "Smart Cloud Strategy (May 2010)," (presented at NIST "Cloud Computing Forum & Workshop, June 5-7, 2012, Washington DC), p. 1, http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ForumVAgenda/2_Smart_Cloud_Strategy_of_Japan_Yasuo_Sakamoto.pdf.

[iv] Daniel Mason, "EU says Cloud Computing a 'game changer' for economy," *Public Service Europe*, September 27, 2012, http://www.publicserviceeurope.com/article/2511/eu-says-cloud-computing-a-game-changer-for-economy.

[v] European Commission, "Unleashing the Potential of the Cloud in Europe," COM(2012) 529, Brussels, 27.9.2012, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

[vi] European Commission, "Unleashing the Potential of the Cloud in Europe," (2012), pp. 5-6.

[vii] We use the term "government" in a broad sense, encompassing not only government agencies and other units of the (typically centralized) executive branch, but also other publicly funded institutions, including for public schools, hospitals, and similar entities established within the framework of public law and funding, as such entities are often at the forefront when adopting cloud technologies and solutions.

[viii] Established by law, the Council is the "principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of the Federal Government information resources." 44 U.S.C. § 3603. The CIO Council includes a number of key officials from important agencies such as the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, State, Transportation, the Treasury, Veterans Affairs, the Army, the Navy, the Air Force, and the Environmental Protection Agency, and the National Aeronautics and Space Administration.

[ix] Vivek Kundra, US Chief Information Officer, "Federal Cloud Computing Strategy," US Office of Management and Budget (February 8, 2011), p. 2.

[x] *See, e.g.*, US NIST, "NIST Cloud Computing Related Publications," http://nist.gov/itl/cloud/publications.cfm (last accessed June 22, 2013); US Department of Homeland Security (DHS), "Cybersecurity Results," http://www.dhs.gov/cybersecurity-results, (last accessed June 22, 2013) (noting DHS interagency partnerships across the US government); US General Services Administration (GSA), "Cloud IT Services," http://www.gsa.gov/portal/category/100671 (last accessed June 22, 2013).

[xi] *See, e.g.*, "European Commission launches cloud computing consultation," *Computer Weekly*, May 17, 2011, http://www.computerweekly.com/news/1280095890/European-Commission-launches-cloud-computing-consultation; Kevin J. O'Brien, "Cloud Computing Hits Snag in Europe," *New York Times*, September 19, 2010, http://www.nytimes.com/2010/09/20/technology/20cloud.html.

[xii] Daniel Mason, "EU says Cloud Computing a 'game changer' for economy," *Public Service Europe*, September 27, 2012, http://www.publicserviceeurope.com/article/2511/eu-says-cloud-computing-a-game-changer-for-economy. *See also* European Commission, "Unleashing the Potential of the Cloud in Europe," (2012).
[xiii] European Commission (EC), "Unleashing the Potential of the Cloud in Europe," COM(2012) 529, Brussels, September 27, 2012, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.
[xiv] *Id*.
[xv] *Id*.
[xvi] UK Government, Cabinet Office, "Government ICT Strategy," March 2011, p. 4, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-government-government-ict-strategy_0.pdf.
[xvii] Kathleen Hall, "CIO Interview: Andy Nelson, UK government chief information officer," *Computer Weekly*, April 26, 2012, http://www.computerweekly.com/news/2240149128/CIO-interview-Andy-Nelson-government-IT-head.
[xviii] UK Government, "Government Cloud Strategy," (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85982/government-cloud-strategy_0.pdf.
[xix] UK Government, Cabinet Office, "One Year On: Implementing the Government ICT Strategy," May 2012, https://www.gov.uk/government/publications/one-year-on-implementing-the-government-ict-strategy.
[xx] Sakamoto, "Smart Cloud Strategy (May 2010)," (2012), p. 1.
[xxi] *Id*.
[xxii] Forbes, Cloud Could Cut $12 Billion from US Government Annual Deficit (April 2012), http://www.forbes.com/sites/joemckendrick/2012/04/30/cloud-could-cut-12-billion-from-us-government-annual-deficit-study/
[xxiii] UK, "Government Cloud Strategy," (2011), p. 16. For a detailed breakdown of these projections, *see* HM Government, "G-Cloud – Savings," August 20, 2012, http://gcloud.civilservice.gov.uk/about/savings.
[xxiv] US CIO, "Federal Cloud Computing Strategy," (2011).; Mike Barton, "Cloud saves Feds $5B a Year, Study Finds," *Wired*, May 1, 2012, http://www.wired.com/cloudline/2012/05/cloud-fed-savings/.
[xxv] John Foley, "Claims of Government Cloud Savings Don't Add Up," *Information Week*, April 9, 2012, http://www.informationweek.com/government/cloud-saas/claims-of-government-cloud-savings-dont/224202488.
[xxvi] UK, "Government Cloud Strategy," (2011).
[xxvii] Sakamoto, "Smart Cloud Strategy (May 2010)," (2012).
[xxviii] US CIO, "Federal Cloud Computing Strategy," (2011).
[xxix] European Commission, "Unleashing the Potential of the Cloud in Europe," (2012).
[xxx] IDC EMEA, "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take," SMART 2011/0045, July 13, 2012 (report conducted on behalf of European Commission), http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf.
[xxxi] Sakamoto, "Smart Cloud Strategy (May 2010)," (2012)..
[xxxii] UK, "Government ICT Strategy," (2011).
[xxxiii] US Government Accountability Office (GAO), "Information Security: Additional Guidance Needed to Address Cloud Computing Concerns," GAO-12-130T, October 6, 2011, http://www.gao.gov/assets/590/585638.pdf.
[xxxiv] *Id*.
[xxxv] European Commission, "Unleashing the Potential of the Cloud – Commission Staff Working Document," SWD(2012) 271 Final, Brussels, September 27, 2012, p. 10, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF.
[xxxvi] ENISA (2012), "Procure Secure – a guide to monitoring of security service levels in cloud contracts" 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts. .
[xxxvii] *Cf.* US NIST, "The NIST Definition of Cloud Computing," (2011). It's worth noting that a cross-cutting model called "community cloud" also exists. In this model, cloud infrastructure is provisioned for use by a community of related organizations, and may be owned and operated by a community member or a third-party service provider.
[xxxviii] It should be emphasized that giving the government greater control over security does not guarantee better or greater degree of security. Some scholars have pointed out that public cloud services can in some cases provide more effective security, due in part to the expertise and experience of the service provider, than a privately owned and operated cloud service. *See, e.g.*, Terrence August, Marius Florin Niculescu, and Hyoduk Shin, "Cloud Computing: Impactions on Network Structure and Security Risks" (September 11, 2011), http://ssrn.com/abstract=1933618.

[xxxix] US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012), p. 16.
[xl] *Id*.
[xli] *Id*., p. 15.
[xlii] *Id*., p. 18.
[xliii] US Government Accountability Office (GAO), "Information Technology: OMB and Agencies Need to Fully Implement Major Initiatives to Save Billions of Dollars," GAO-13-297T, January 22, 2013, http://www.gao.gov/assets/660/651376.pdf; US Government Accountability Office (GAO), "Information Technology Reform: Progress Made; More Needs to Be Done to Complete Actions and Measure Results," GAO-12-461, April 2012, http://www.gao.gov/assets/600/590457.pdf.
[xliv] European Commission, "Unleashing the Potential of the Cloud – Commission Staff Working Document," (2012), p. 10.
[xlv] *See, e.g.*, Michael Hettinger, "Move to cloud requires new, different thinking," *Federal Times*, August 5, 2012, http://www.federaltimes.com/article/20120805/ADOP06/308050004/Move-cloud-requires-new-different-thinking.
[xlvi] US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012), p. 19.
[xlvii] W. Kuan Hon, Christopher Millard, Ian Walden, "UK G-Cloud v1 and the Impact on Cloud Contracts," April 11, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038557.
[xlviii] *Id*.
[xlix] *See* Gavin Clarke, "Is it all over for UK.gov's G-Cloud 3.0? A footnote in history awaits," *The Register*, December 4, 2012, http://www.theregister.co.uk/2012/12/04/end_of_g_cloud/; *see also* Queen Mary University of London, Cloud Legal Project, "UK G-Cloud V1 – liability provisions – evolution," http://www.cloudlegal.ccls.qmul.ac.uk/Research/researchpapers/71492.html.
[l] FedRAMP, http://fedramp.gov/ (last accessed June 22, 2013).
[li] *See* J. Nicholas Hoover, "Feds Issue First Cloud Services Security Authorization," *Information Week*, December 28, 2012, http://www.informationweek.com/government/cloud-saas/feds-issue-first-cloud-services-security/240145353.
[lii] FedRAMP Compliant CSPs, http://www.gsa.gov/portal/content/131931.
[liii] Derek du Preez, "Deputy CIO promises to improve G-Cloud accreditation processes," *Computer World UK*, November 29, 2012, http://www.computerworlduk.com/news/public-sector/3413782/deputy-gov-cio-promises-to-improve-g-cloud-accreditation-processes/.
[liv] US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012), p. 20.
[lv] Steve Towns, "Federal Web Portal Moves to Cloud Computing Platform," *Government Technology*, May 1, 2009, http://www.govtech.com/pcio/Federal-Web-Portal-Moves.html.
[lvi] UK Cabinet Office, "Government Cloud Strategy," p. 19.
[lvii] US CIO, "Federal Cloud Computing Strategy," (2011)..
[lviii] US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012).
[lix] UK Cabinet Office, "Government Cloud Strategy," (2011), p. 5.
[lx] US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012), p. 19.
[lxi] *Id*., p. 19.
[lxii] *See, e.g.*, Chris Reed, "Information 'Ownership' in the Cloud," *Queen Mary School of Law Legal Studies Research Paper No.45/2010* (March 2, 2010), http://ssrn.com/abstract=1562461.
[lxiii] *See, e.g.*, Barb Darrow, "Fear of lock-in dampens cloud adoption," *GigaOm* February 26, 2013, http://gigaom.com/2013/02/26/fear-of-lock-in-dampens-cloud-adoption/. For a general overview, *see* Urs Gasser, John Palfrey, and Matthew Becker, "Mapping Cloud Interoperability in the Globalized Economy: Theory and Observation from Practice," *Berkman center Research Publication No. 2012-19* (June 1, 2012), http://ssrn.com/abstract=2192641.
[lxiv] US CIO, "Federal Cloud Computing Strategy," (2011), p. 15; UK Cabinet Office, "Government Cloud Strategy," (2011), p. 15; European Commission, "Unleashing the Potential of Cloud Computing in Europe," (2012), pp. 10-14.
[lxv] Ian Walden and Lise Da Corregio Luciano, "Ensuring Competition in the Clouds: The Role of Competition Law?," *Queen Mary School of Law Cloud Legal Research Project* (April 17, 2011), http://ssrn.com/abstract=1840547.

[lxvi] US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012), p. 19.
[lxvii] *See, e.g.*, European Commission, "Unleashing the Potential of the Cloud in Europe," (2012). *See also* Urs Gasser, John Palfrey, and Matthew Becker, "Mapping Cloud Interoperability in the Globalized Economy: Theory and Observation from Practice," *Berkman center Research Publication No. 2012-19* (June 1, 2012), http://ssrn.com/abstract=2192641.
[lxviii] The Cloud Project Legal Team at the Queen Mary School of Law has published a number of excellent papers exploring the dimensions of this problem in the context of Europe. *See, e.g.*, W. Kuan Hon and Christopher Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing Part 4, *Queen Mary School of Law Legal Studies Research Paper No. 85/2011* (April 4, 2012), http://ssrn.com/abstract=2034286; W. Kuan Hon, Julia Hörnle, and Christopher Millard, "Data Project Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3," *International Review of Law, Computers & Technology*, vol. 26, no. 2-3 (2012), http://ssrn.com/abstract=1924240.
[lxix] European Parliament, "Cloud Computing Study," IP/A/IMCO/ST/2011-18 (May 2012), pp. 45-47, http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=73411.
[lxx] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe,'" November 16, 2012, pp. 5-8, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.
[lxxi] *See, e.g.*, W. Kuan Hon, Julia Hörnle, Christopher Millard, "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law?, February 9, 2012, http://ssrn.com/abstract=1783577.
[lxxii] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe,'" (2012), pp. 9-13.
[lxxiii] Paolo Balboni, "Data Protection and Data Security Issues Related to Cloud Computing in the EU," *ISSE 2010 Securing Electronic Business Processes – Highlights of the Information Security Solutions Conference 2010* (August 18, 2010), http://ssrn.com/abstract=1661437.
[lxxiv] Often criticized for its age and ill-application to new technology, the Electronic Communication Privacy Act (ECPA) provides a series of protections against access by the government of information related to private communications facilitated by through third-party mediums. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2712. Recently, legislators have introduced new proposals to updates these laws in response to technological developments like cloud computing. *See, e.g.*, Electronic Communications Privacy Act Amendments of 2013, S. 607, 113th Cong. (2013-2014), text available at http://beta.congress.gov/bill/113th-congress/senate-bill/607.
[lxxv] *See, e.g.*, European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Brussels, 25.1.2012, COM(2012) 11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. ;
[lxxvi] EC, "Unleashing the Potential of the Cloud in Europe," (2012); European Commission, Article 29 Working Party, "Opinion 05/2012 on Cloud Computing," 01037/12/EN, WP 196, adopted 1 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf; European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe,'" November 16, 2012, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.
[lxxvii] "Unleashing the Potential of the Cloud in Europe," (2012).
[lxxviii] *Cf.* Herbert Burkert and Urs Gasser, "Regulating Technological Innovation: An Information and a Business Law Perspective" in *Rechtliche Rahmenbedingungen des Wirtschaftsstandortes Schweiz: Festschrift 25 Jahre juristische Abschlüsse an der Universität St. Gallen* (Zurich: Dike, 2007), pp. 503-523.
[lxxix] *Cartoon Network LP v. CSC Holdings*, 536 F.3d 121 (2d Cir. 2008); *Twentieth Century Fox Film Co. v. Cablevision Systems Corp.*, 478 F.Supp.2d 607 (SDNY 2007).
[lxxx] *See* Vince Veneziani, "Store Music Online In Japan, Get Arrested," *Tech Crunch*, May 29, 2007, http://techcrunch.com/2007/05/29/store-music-online-in-japan-get-arrested.

[lxxxi] *Cf.* Deborah L. Spar, *Ruling the Waves* (Harcourt: New York, 2001).
[lxxxii] *See, e.g.*, Electronic Communications Privacy Act Amendments of 2013, S. 607, 113th Cong. (2013-2014), text available at http://beta.congress.gov/bill/113th-congress/senate-bill/607. *See also* European Commission, "Commission proposes a comprehensive reform of data protection rules," Press Release, January 25, 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[lxxxiii] This is a key feature of the UK Government's ICT and cloud strategies, which emphasize that "the Government will also put an end to the oligopoly of large suppliers that monopolise its ICT provision" and "remove barriers to allow SMEs, the voluntary and community sector and social enterprise to participate in the ICT marketplace." UK Government, Cabinet Office, "Government Cloud Strategy," 2011, pp. 8-10.
[lxxxiv] Google, for example, has been the target of several antitrust investigations involving regulators in the US and Europe. *See, e.g.*, James Kanter and Claire Miller, "In European Antitrust Fight, Google Needs to Appease Competitors," *New York Times*, July 17, 2013, http://www.nytimes.com/2013/07/18/technology/europe-wants-more-concessions-from-google.html; Edward Wyatt, "F.T.C. Is Said to Begin a New Inquiry on Google," *New York Times*, May 24, 2013, http://www.nytimes.com/2013/05/25/technology/ftc-said-to-have-begun-new-inquiry-on-google.html.
[lxxxv] In EU, see recent efforts by European Commission related to breach notifications. European Commission, "Digital Agenda: New specific rules for consumers when telecoms personal data is lost or stolen in EU," Press Release, June 24, 2013, http://europa.eu/rapid/press-release_IP-13-591_en.htm. Breach notification laws in the US are enacted by state, and by sector-specific regulations. *See, e.g.*, Massachusetts General Laws, ch. 93H, §§ 1-6; Health and Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009).
[lxxxvi] Cloud Computing Act of 2012, S. 3569 ,112th (2011-2012), http://beta.congress.gov/bill/112th/senate-bill/3569/text.
[lxxxvii] NIST, "Cloud Computing Program," http://www.nist.gov/itl/cloud/.
[lxxxviii] NIST, "Standards Acceleration to Jumpstart the Adoption of Cloud Computing," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/SAJACC (last accessed June 22, 2013).
[lxxxix] NIST, "Standards Roadmap," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsRoadmap (last accessed June 22, 2013).
[xc] NIST, "Press Release: NIST Helps Accelerate the Federal Government's Move to the Cloud," June 9, 2010, http://www.nist.gov/itl/csd/cloud_060910.cfm. *See also* NIST, "Cloud Security," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity (last accessed June 22, 2013); NIST, "Federal Risk and Authorization Management Program (FedRAMP)," http://www.nist.gov/itl/cloud/fedramp.cfm (last accessed June 22, 2013).
[xci] European Commission, "Unleashing the Potential of the Cloud – Commission Staff Working Document," (2012).
[xcii] *Id*., p. 10.
[xciii] *Id*.
[xciv] *Id*., pp. 10-11.
[xcv] *Id*., p. 29.
[xcvi] Global Inter-Cloud Technology Forum, http://www.gictf.jp/index_e.html (last accessed June 22, 2013).
[xcvii] European Commission, "Unleashing the Potential of the Cloud – Commission Staff Working Document," (2012), pp. 13-14.
[xcviii] European Commission, "Establishing a European Cloud Partnership to Drive Innovation and Growth from the Public Sector," January 26, 2012, http://europa.eu/rapid/press-release_SPEECH-12-38_en.htm?locale=en.
[xcix] European Commission, "Digital Agenda: Tech CEOs and leaders kickstart new EU cloud computing board", November 19, 2012, http://europa.eu/rapid/press-release_IP-12-1225_en.htm.
[c] SIENA, http://www.sienainitiative.eu/ (last accessed June 22, 2013).
[ci] SIENA, "SIENA Roadmap," http://www.sienainitiative.eu/Pages/Static.aspx?id_documento=77e47efb-7b89-4b20-aa1b-ea1a60ef5c08 (last accessed June 22, 2013).
[cii] Ministry of Internal Affairs and Communications, "Cloud Testbed Consortium Established," December 16, 2011, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/11121604.html.
[ciii] John Palfrey and Urs Gasser, *Interop – the promise and perils of highly interconnected systems* (Basic Books: New York, 2012).
[civ] *See, e.g.*, Barb Darrow, "Fear of lock-in dampens cloud adoption," *GigaOm* February 26, 2013, http://gigaom.com/2013/02/26/fear-of-lock-in-dampens-cloud-adoption/; Quentin Hardy, "Open vs. Closed: The

Cloud Wars," *New York Times*, October 9, 2012, http://bits.blogs.nytimes.com/2012/10/09/open-vs-closed-the-cloud-wars/. For a general overview, *see* Urs Gasser, John Palfrey, and Matthew Becker, "Mapping Cloud Interoperability in the Globalized Economy: Theory and Observation from Practice," *Berkman center Research Publication No. 2012-19* (June 1, 2012), http://ssrn.com/abstract=2192641.

[cv] Stacy Baird, "The Government at the Standards Bazaar," *Stanford Law and Policy Review*, vol. 18, pp. 35-99 (2007).

[cvi] European Commission, "Unleashing the Potential of the Cloud – Commission Staff Working Document," (2012), p. 26.

[cvii] Committee on Innovations in Computing and Communications: Lessons from History, National Research Council, *Funding a Revolution: Government Support for Computing Research* (Washington, DC: National Academy of Sciences 1999), pg. 138-9.

[cviii] *See, e.g.*, Marjorie Censer, "The country's CIO says a fourth of federal IT spending can be shifted to the cloud," *Washington Post*, February 21, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/18/AR2011021805784.html; Sean Collins Walsh, "Federal Push for 'Cloud' Technology Faces Skepticism," *New York Times*, August 21, 2011, http://www.nytimes.com/2011/08/22/technology/federal-push-for-cloud-technology-faces-skepticism.html.

[cix] Sean Collins Walsh, "Federal Push for 'Cloud' Technology Faces Skepticism," *New York Times*, August 21, 2011, http://www.nytimes.com/2011/08/22/technology/federal-push-for-cloud-technology-faces-skepticism.html.

[cx] Marjorie Censer, "The country's CIO says a fourth of federal IT spending can be shifted to the cloud," *Washington Post*, February 21, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/18/AR2011021805784.html.

[cxi] Kathleen Hall, "Cloud Computing will become the government's 'common infrastructure', says Francis Maude," *Computer Weekly*, October 27, 2011, http://www.computerweekly.com/news/2240106275/Cloud-computing-will-become-the-governments-common-infrastructure-says-Francis-Maude.

[cxii] Info.Apps.Gov, http://info.apps.gov/ (last accessed June 22, 2013).

[cxiii] "Federal Case Studies," http://info.apps.gov/content/federal-cloud-computing-case-studies.

[cxiv] *See, e.g.*, GSA, "Ordering Guide – Infrastructure as a Service," 2012, https://info.apps.gov/sites/default/files/IaaS%20Ordering%20Guide%20v4%206_10052012.pdf.

[cxv] Florence de Borja, "Cloud Computing Companies Get Funding in France," *Cloud Times*, September 19, 2012, http://cloudtimes.org/2012/09/19/cloud-funding-france/.

[cxvi] Derek du Preez, "Government launches £40m fund to support cloud SMEs," *Computer World UK*, April 17, 2012, http://www.computerworlduk.com/news/public-sector/3351718/government-launches-40m-fund-to-support-cloud-computing-smes/.

[cxvii] *See, e.g.*, Gartner, "Gartner Says Worldwide Cloud Services Market to Surpass $109 Billion in 2012," September 18, 2012, http://www.gartner.com/it/page.jsp?id=2163616. *But see* Rolf Jester, "When to Stop Using the Cloud Word," *Gartner*, February 13, 2013, http://blogs.gartner.com/rolf-jester/2013/02/13/when-to-stop-using-the-cloud-word.

[cxviii] Cicely K. Dyson, "Can the Cloud Help Small Businesses?," *Wall Street Journal*, January 9, 2013, http://online.wsj.com/article/SB10001424127887323706704578230641145851624.html.

[cxix] Vivek Kundra, US CIO, "25 Point Implementation Plan to Reform Federal Information Technology Management," December 9, 2010, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA543512.

[cxx] NIST, Cloud Computing Program, http://www.nist.gov/itl/cloud/ (last accessed June 22, 2013).

[cxxi] NIST, "Useful Documents for Cloud Adopters," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/Documents (last accessed June 22, 2013).

[cxxii] European Commission, "Unleashing the Potential of the Cloud in Europe," (2012).

[cxxiii] National Science Foundation, "NSF Report on Support for Cloud Computing," 2012, http://www.nsf.gov/pubs/2012/nsf12040/nsf12040.pdf. *See also* National Science Foundation, "The Sky Is No Limit: 13 Research Teams Compete in the Clouds," Press Release 11-082, April 20, 2011, http://www.nsf.gov/news/news_summ.jsp?org=NSF&cntn_id=119248&preview=false.

[cxxiv] National Science Foundation, "The Sky Is No Limit: 13 Research Teams Compete in the Clouds," Press Release 11-082, April 20, 2011, http://www.nsf.gov/news/news_summ.jsp?org=NSF&cntn_id=119248&preview=false.

[cxxv] European Commission, "FP7 in Brief," 2007, http://ec.europa.eu/research/fp7/pdf/fp7-inbrief_en.pdf.

[cxxvi] *Id*.

[cxxvii] *See, e.g.*, European Commission, "Cloud Computing Related Research," January 2012, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/cloudcomputing_related_research_20120112_full.pdf.
[cxxviii] Federal Ministry of Economics and Technology, "The Standardisation Environment for Cloud Computing," http://www.bmwi.de/English/Redaktion/Pdf/normungs-und-standardisierungsumfeld-von-cloud-computing,property=pdf,bereich=bmwi,sprache=en,rwb=true.pdf.
[cxxix] *Id*., p.14.
[cxxx] Sakamoto, "Smart Cloud Strategy (May 2010)," (2012).
[cxxxi] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," NIST Special Pubication 800-145 (September 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[cxxxii] Cloud Computing Act of 2012, S. 3569 ,112th (2011-2012), http://beta.congress.gov/bill/112th/senate-bill/3569/text.
[cxxxiii] Eric Goldman, "The Proposed 'Cloud Computing Act of 2012,' and How Internet Regulation Can Go Awry," *Technology & Market Law Blog*, October 11, 2012, http://blog.ericgoldman.org/archives/2012/10/the_proposed_cl.htm.
[cxxxiv] *See* US GAO, "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," (2012), p. 19.
[cxxxv] Andy Greenberg, "IBM's Chinese Cloud City," *Forbes*, July 28, 2009, http://www.forbes.com/2009/07/27/ibm-china-computing-intelligent-technology-ibm.html.
[cxxxvi]
[cxxxvii] *See, e.g.*, Jeffery B. Liebman, "Building on Recent Advances in Evidence-Based Policymaking," The Brookings Institute (April 2013), http://www.brookings.edu/~/media/research/files/papers/2013/04/17%20liebman%20evidence%20based%20policy/thp_liebmanf2_413.pdf.
[cxxxviii] Arun Chandrasekaran and Mayank Kapoor, "State of Cloud Computing in the Public Sector – A strategic analysis of the business case and overview of initiatives across Asia Pacific," *Frost & Sullivan* (2010), www.frost.com/prod/servlet/cio/232651119.
[cxxxix] *See* Urs Gasser and John Palfrey, "Fostering Innovation and Trade in the Global Information Society: The Different Facets and Roles of Interoperability" in Mira Burri and Thomas Cottier, eds., *Trade Governance in the Digital Age* (New York: Cambridge University Press, 2012), pp.123-153.
[cxl] While it is too early to declare governmental interventions in cloud computing poorly timed, others have pointed to the rich history of unfortunately timed regulatory interventions in other markets. *See, e.g.*, Daniel Gervais, "The Regulation of Inchoate Technologies," 47 *Houston Law Review* 665 (Fall 2010).
[cxli] *See, e.g.*, NIST, "The NIST Cloud Computing Collaboration Site," http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome (last accessed June 22, 2013).
[cxlii] Glenn Greenwald and Ewen MacAskill, "NSA PRISM Program taps in to user data of Apple, Google and others," *The Guardian*, June 6, 2013, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data/print; "US, British intelligence mining data from nine US Internet companies in broad secret program," *Washington Post*, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.
[cxliii] *See, e.g.*, Jordan Novet, "PRISM could foil the public-cloud campaign, and private clouds may lie in crosshairs," *GigaOm*, June 17, 2013, http://gigaom.com/2013/06/17/prism-could-foil-the-public-cloud-campaign-and-private-clouds-might-lie-in-crosshairs/.
[cxliv] *See, e.g.*, Jennifer Baker, "Europe demands PRISM answers from US AG Holder," *Computer World*, June 12, 2013, http://www.computerworld.com/s/article/9239997/Europe_demands_Prism_answers_from_U.S._AG_Holder; Ivor Tossel, "Washington knows what you do online – and Canadians aren't above it," *Globe and Mail*, June 7, 2013, http://www.theglobeandmail.com/commentary/washington-knows-what-you-do-online-and-canadians-arent-above-it/article12407753/.