Irion, Kristina

Conference Paper

Government cloud computing and the policies of data sovereignty

22nd European Regional Conference of the International Telecommunications Society (ITS): "Innovative ICT Applications - Emerging Regulatory, Economic and Policy Issues", Budapest, Hungary, 18th-21st September, 2011

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Irion, Kristina (2011) : Government cloud computing and the policies of data sovereignty, 22nd European Regional Conference of the International Telecommunications Society (ITS): "Innovative ICT Applications - Emerging Regulatory, Economic and Policy Issues", Budapest, Hungary, 18th-21st September, 2011, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/52197

22nd European Regional ITS Conference
Budapest, 18-21 September, 2011

Kristina Irion

GOVERNMENT CLOUD COMPUTING AND THE POLICIES OF DATA SOVEREIGNTY

Abstract

Government cloud services are a new development at the intersection of electronic government and cloud computing which holds the promise of rendering government service delivery more effective and efficient. Cloud services are virtual, dynamic and potentially stateless which has triggered governments' concern about data sovereignty. This paper explores data sovereignty in relation to government cloud services and how national strategies and international policy evolve. It concludes that for countries data sovereignty presents a legal risk which can not be adequately addressed with technology or through contractual arrangements alone. Governments therefore adopt strategies to retain exclusive jurisdiction over government information

JEL codes H11, H73, H83
Keywords cloud computing, electronic government, data sovereignty, data ownership, information assurance, international data transfers

Authors' affiliation and corresponding author's e-mail address
Dr. Kristina Irion
Assistant Professor, Department of Public Policy
Research Director, Public Policy, at the Center for Media and Communications Studies (CMCS)
Central European University
Nador utca 9, H-1051 Budapest
Email irionk@ceu.hu

Introduction

Two major trends in information and communications technology (ICT) merge: First, the public sector is embarking on electronic government solutions for its back-office operations. Second, cloud computing is fundamentally changing the way how computing is done by providing ubiquitous, on-demand access to computing resources. Government cloud services hold the promise of rendering government service delivery and back-office operations more effective and efficient. What looks like an ideal match actually raises a range of unresolved issues.

Electronic government describes the use of information and communication technologies (ICT) in the public sector. Mayer-Schönberger and Lazer state that "[t]he purpose of electronic government is similar to the use of all information-handling technologies before: to save public resources and to make public-sector activity more efficient." (2007, 4). Cloud computing holds the promise of rendering government service delivery more effective and efficient while providing a platform for open government, inter-agency cooperation and government innovation.

When "information is the foundation of all governing" (Mayer-Schönberger and Lazer 2007, 1) than the modern treasury of public institutions is where the wealth of public information is stored and processed. Government in most countries is under very strict obligations to ensure that public IT systems and information are secure. However, cloud services have been characterized as virtual, dynamic and potentially stateless (NIST 2009) taking information government to "a new level of abstraction" (Petersen, Gondree, and Beverly 2011, 1).

Against this backdrop, many governments have raised the concern about data sovereignty when government information are moved to the cloud. How to ensure confidentiality, integrity and availability of public assets residing in the cloud? What if public information and IT systems are hosted abroad? Is government data of one country caught under the authority of another jurisdiction and what are the resulting risks? The concept of data sovereignty essentially frames this scenario and seeks to compensate for the progressing virtualization of information where digital data is stored and processed remotely.

The public policy challenges of cloud computing have already attracted academic attention mainly with regards to the shortcomings of the present regulatory frameworks, international inconsistencies and the need for an enabling environment for cloud services. Jaeger, Lin and Grimes (2008) opened the discussion of information policy issues of cloud computing pertaining to privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and

liability. In his paper Nelson (2009) focuses on governments' role in fostering portability, competition and innovation in cloud services. Reed's paper (2010) is discussing information "ownership" with respect to cloud services well acknowledging that property rights in information do not exist. Kushida, Murray and Zysman (2011) convey the core aspects of the cloud computing service markets with a view on the influence policy issues take on their development. As a burgeoning market and the next hype corporations, analysts and pundits discuss the national and international policy issues addressing policy makers with varying sets of recommendations (Microsoft Corporation 2010; Rayport and Heyward 2009; World Economic Forum, hereinafter WEF, 2011).

There are a handful of studies on government cloud service mostly from the US that focus on the cost economies and challenges for governments' IT migration to cloud services. The most comprehensive study to date by Wyld (2009) identifies ten major challenges facing government in implementing cloud computing that are technical, regulatory and organizational. His subsequent survey examines the adoption of government cloud service from an international perspective and what this means for public IT professionals (Wyld 2010). West (2010a) deals in one study with cost economies from government cloud services in which he analyzes available data. In the second study, he provides policy guidance to improve cloud computing in the public sector (West 2010b). Existing policy documents provide an additional source of information since national cloud computing strategies for the public sector are conclusive about the motivations, objectives and transition paths to government cloud services.[1] Data sovereignty is a notion which has been raised mainly in the context of government cloud services, but there has been no attempt to define and analyze this concept in the literature so far.

This paper explores data sovereignty in relation to government cloud services and how national strategies and international policy evolve. It brings the various strands of literature on electronic government, public policy of cloud computing, and of government cloud services together. The paper contributes to the state of research in proposing a definition of data sovereignty for the purpose of electronic government and when it discusses the pertaining public policy problem. The cloud computing strategies of Australia, Canada, the United Kingdom and the United States will be introduced and analyzed with a view on safeguarding data sovereignty. It will finally explore the argument if international agreements or European Union integration can address data sovereignty of government data in the clouds. The paper does not attempt to investigate the wider landscape of technical security and data protection in government cloud services.

[1] *See* Section on Comparative Analysis of National Cloud Computing Strategies.

This paper is structured as follows: The first section provides a concise introduction to cloud computing followed in section two by an overview over government cloud services and arguments. The third section turns to data sovereignty and how this concept is derived. The forth section delivers the comparative analysis of national cloud computing strategies of the four countries. The last section discusses the role of international policy and the European Union strategy for an internal digital market followed by the conclusions.

About cloud computing

Cloud computing is often referred to as the next paradigm shift in networked computing because it brings about computing on demand (Jaeger, Lin, and Grimes 2008, 271; Rayport and Heyward 2009, ii, 3). In short, cloud technology overhauls traditional methods of computing where data is stored and software is run on decentralized equipment such as a desk-top computer or a local server. Instead, applications and data are moved to shared data centers (Kushida, Murray, and Zysman 2011, 4), in what technologists have dubbed "the cloud" – i.e. powerful computing platforms which can be accessed remotely and where data resides and computing is performed. It is important to note that in the cloud scenario the third party which owns and maintains the infrastructure also controls data and applications (Jaeger, Lin, and Grimes 2008, 272). This positions cloud operators as a distinct type of internet intermediaries with their own eclectic range of policy challenges.

Cloud computing has emerged as a result of a number of technological advances, notably (1) broadband connectivity, (2) commodity server hardware with open interfaces, (3) open source software for operating systems, web servers and distributed computing, and (4) open standards in Web 2.0 applications (Australian Government Department of Finance and Deregulation 2011, 11; Nelson 2009, 3). The know-how for distributed computing and the operation of large data centers has developed in the commercial sector in order to handle data and processing intensive services. This is particularly true of web services such as search engines which process a myriad of queries and online shops where concurrent transactions are processed (Jaeger, Lin, and Grimes 2008, 271). Internet and IT companies such as Amazon, Google, IBM and Microsoft are among today's largest cloud service providers but there are increasingly new entrants, such as Salesforce. Open standards and open source software centrally buttress the development of the cloud infrastructure, which infused interoperability and slashes the costs of software.

In the literature various definitions are proposed, yet most widely cited is that of the National Institute of Standards and Technology (hereafter NIST). Thereafter, "[c]loud computing is a model for enabling 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." (NIST 2009) This definition is composed of five characteristics which are in short revisited. First, as an on-demand service users can "unilaterally provision computing capabilities […] as needed automatically" (NIST 2009). Second, the cloud service can be accessed via broadband network and standard protocols which support heterogeneous clients and user equipment (NIST 2009). Third, resources are pooled to provision multiple users' demands with physical and virtual resources, for instance storage, processing, memory, network bandwidth, and virtual machines (NIST 2009). Fourth, "capabilities can be rapidly and elastically provisioned" (NIST 2009) in order to meet demand lows and peaks as required by the users. Fifth, the use of the service is automatically measured in an abstract unit, for example storage, processing or bandwidth (NIST 2009), based on which the utilized service is billable.

Cloud computing "alters the basic economics of access to computing and storage" (Rayport, and Heyward 2009, ii). Through the aggregation and consolidation of computing needs cloud operators can realize economies of scale which significantly reduces the operation costs of data centers (Kushida, Murray, and Zysman 2011, 2). It is important to note that there is not just one cloud but many and that operators vary in size; however, it is well established that scale economies favor size. Kushida, Murray and Zysman observe that "[t]he full economic promise of cloud computing depends on the ability to attain truly massive scale, delivering global-scale services that transcend traditional political and economic boundaries." (2011, 3) The flexible provision, the metered use and the consumption-based pricing models have prompted comparisons to other utility services (Jaeger, Lin, and Grimes 2008, 271; Kushida, Murray, and Zysman 2011, 4; Wyld 2009, 56). Yet, the traditional concept of what is a utility service does not fit entirely because cloud capacity is not simply a commodity but can be customized to support varying functionalities (Kushida, Murray, and Zysman 2011, 4). Notwithstanding, it could develop into an utility of its own kind.

Virtually anybody and anything from every possible background ranging from individuals to companies of all sizes, public, private and not-for profit organizations, universities and research centers etc. can use cloud services. Many popular Internet and Web 2.0 services of today bear characteristics of cloud services whether users store files, share photos, send tweets, update a profile on a social network, use web applications or collaborate online. Apart from benefiting from lower prices users of cloud services avoid upfront investments in local ICT infrastructure and software, skip most in-house IT management and, instead, pay for exactly the computing capacity they utilize (Jaeger, Lin, and Grimes 2008, 271f.; Nelson 2009, 3f.). The flexible provision of cloud computing can give businesses a competitive edge, faster time to market and even scalable services in order to meet their customers' actual

demand. The expectations and needs of users greatly vary depending on the context and preferences.

Once cloud services mature and are widely adopted its inherent transformative power is predicted to benefit society at large. Access to cloud technology releases new capabilities for innovation and entrepreneurship, it faciliates market entry, scalability of operations and experimentation (Kushida, Murray, and Zysman 2011, 2). Processing intensive tasks and applications can now be easily outsourced and powerful computing resources become for the first time publicly accessible. In the hand of researchers the available computing power enables them to tackle computationally-intensive problems and models from all disciplines (Nelson 2009, 4). It further presents an ideal infrastructure for collaboration in the research, private and public sector by offering a shared pool of resources to a community of users. Last but not least, cloud computing is put forward as a green ICT which helps reduce energy consumption by consolidating data centers and enhancing energetic efficiency while bringing down overcapacities (OECD 2010b, 22; Rayport and Heyward 2009, 42).

Following the NIST taxonomy four different models of cloud computing are commonly deployed. The private cloud is an infrastructure which is operated exclusively for one client or organization which is managed either by the organization itself or on behalf of it by a third party (NIST 2009). A community cloud is a shared infrastructure with a common framework that supports a specific community managed by the organizations or a third party (NIST 2009). A public cloud infrastructure "is made available to the general public or a large industry group and is owned by an organization selling cloud services." (NIST 2009) Finally, the hybrid cloud combines two or more clouds (private, community, or public) that remain unique entities but share some infrastructure, for example to balance the load between the clouds (NIST 2009). In all cases it does not matter where the data center is physically located; however, mainly for security reasons the private and the community cloud infrastructure are often kept on premise. Further distinctions and assessment models can be used to describe various types of clouds under technical and commercial aspects.[2] For the purpose of this paper it it sufficient to understand that cloud services are ***virtual***, ***dynamic*** and potentially ***stateless*** (NIST 2009).

Government cloud services

The substantial promise of cloud services meets the pronounced interest of many governments worldwide which are conscious about how they spend taxpayers money and are keenly seeking ways how to do more with less (Wyld 2009, 20). The public sector is very large and sometimes is even the biggest user of ICT in a given country;

[2] For a taxonomy of cloud services *see* Kushida, Murray, and Zysman 2011; Nelson 2009.

centralizing government's computational needs can leverage significant economies of scale. In most countries the public ICT infrastructure, however, replicates government organization with many dispersed data centers serving the needs of specific government departments. Additionally, the server utilization has been reportedly low - sometimes as low as seven percent - keeping generous contingencies with the consequence that massive overcapacity are left unexploited (The Brookings Institution 2010, 3, 6). Government cloud services promise to overcome this fragmentation by consolidating data centers and using storage space more effectively.

The most immediate objective of government cloud strategies is to increase effectiveness and efficiency of administrative processes (Kundra 2010, 9). Wyld identifies governments' need to save public resources to be one of the main drivers of government cloud services' take-up (2009, 10f.). Analysts predicted for the US that moving public sector operations to cloud services could eventually save from 65 to 85 percent of federal agencies' yearly ICT budgets (Booz Allen Hamilton 2009, 5). Although most estimates concur with the finding that government cloud services will curb public spending in IT services the prognosticated savings vary considerably (West 2010a, 2f.). West points out that the cost economies are determined by many factors, such as how extensive the migration is, which type of cloud is deployed and the level of security sought (2010a, 3f.). On a cautionary note, a 2009 report disputed these cost savings for large entities altogether (McKinsey 2009). It maintains that compared to large enterprise data centers, current cloud computing offerings are not *per se* more cost-effective (McKinsey 2009). Some customized features of cloud service such as exclusivity and enhanced security drive up the operational costs compared to the most basic offerings. Given the uncertainties and the complexity surrounding cost economies, governments are well advised to conduct a thorough cost-benefit-analysis.

Beyond the possible financial upside cloud computing carries a number of attractive promises for the public sector. Through cloud services the otherwise expensive and time consuming IT systems administration is essentially outsourced. For the public sector which has arguably difficulties competing for skilled personnel and maintaining state of the art IT systems, this may come at the very least as a relief, if not a rescue (Nelson 2009, 4). Because it is a remotely accessible on-demand service cloud computing overcomes the locational imperative which plays out in two important ways. First, countries can potentially procure services on an international scale. Nelson (2009, 4) asserts that developing countries can access via the cloud the latest computing technologies provided they have an adequate Internet infrastructure at avail. At the level of the infrastructure it does not matter whether the required broadband networks are fixed or wireless; however, where countries or regions are excluded from cloud services for reasons of bandwidth, the digital divide between the developed and the developing world deepens. Second, cloud computing further

reduces the locational imperative in the organization of the public sector (Mayer-Schönberger and Lazer 2007, 7) which could be transformed considering different objectives, for example the decentralization of government and public services.

As a tool of electronic government cloud computing can facilitate the enhanced transparency aspired to in a modern democratic society. According to Kundra, the US Federal Chief Information Officer, it is the ideal platform for the movement of open data wherein the government democratizes its data (The Brookings Institute 2010, 14) and shares it with the public. Ultimately, the whole process of governance can become more transparent and inclusive while enhancing the deliberative capacity of public institutions by admitting stakeholders to follow and to contribute to policy formulation. Note that in line with the prevalent electronic government discourse a technology alone does not transform government (Mayer-Schönberger and Lazer 2007, 4f.) but it is upon the government to yield these results or, conversely, to confine the implementation of a technology to merely an efficiency enhancing measure.

Also within government cloud computing is believed to set free innovative potential "not as a magic wand for solving hard computing and managerial problems" (Nelson 2009, 8) but in the pursuit of enhancing efficiency it eases implementation of many computerized government operations. The collaborative feature of the new platform once fully realized can foster cooperation and collaboration across government departments which may form another source for innovation (Nelson 2009, 8; Rayport and Heyward 2009, 45). Mayer-Schönberger and Lazer (2007, 7) observe that reducing the locational imperative may undermine prevailing organizational structures based on hierarchical principles – the so called information silos. Robinson et al (2010, 46) emphasize the potential to unbundle public services from traditional lines of service delivery. The new environment stimulates what is known as the new public management imperative of networked government which postdates rigid bureaucratic systems and hierarchies (Goldsmith and Eggers 2004, 7). Governmental cloud services can accommodate new interagency collaborative models and new public-private governance networks.

These benefits make a compelling case, but a range of obstacles have to be overcome before government back-offices could embark on this technology. One of the soft factors is that public sector IT management needs to shift mentally from dedicated local infrastructure to a strategy of inclusive government-wide cloud platforms (The Brookings Institution 2009, 8, 38). In practice this is not trivial because consolidation may be resisted by government departments in fear of losing influence, funds, headcount and control. Often the organizational legacy fragments the public sector use of IT with a patchwork of different regulations and procurement formalities (UK Department for Business Innovation and Skills 2009, 211; West 2010b, 5) which need

to be updated first. For instance, Kundra highlights the costly replication of certification procedures in the US where vendors have to "certify their solutions with hundreds of agencies" (The Brookings Institution 2009, 9). Eventually, the migration from legacy systems to government cloud services poses a unique challenge because the various IT systems need to be integrated in order to achieve government-wide utility.

Security is probably the most significant concern that the government shares with other users of cloud computing (Jaeger, Lin, and Grimes 2008, 274; WEF 2011, 8; West 2010b, 6). Government in most countries is under very strict obligations to ensure that public IT systems as well as public information and records are secure.[3] Security is a wide notion which includes all accidental or intentional incidents which may harm the confidentiality, integrity or availability of public resources due to, for example, technical failure or unauthorized access.[4] It is controversial whether government cloud services indeed create a riskier environment compared to local equipment where the perception of security appears to be higher but this is not necessarily true (West 2010b, 6; Wyld 2009, 36f.). Nelson argues in favor of unified cloud infrastructure which is more secure and reliable than "trying to maintain and manage hundreds of different systems" (2009, p. 9; ENISA 2011, 83; Wyld 2009, 36f.).

In fact, governments' security concerns resonate often with the loss of ownership and control in a cloud computing environment where a third party operates the data centers. One fraction of this inhibition has become known as governments' quest for data sovereignty – a burgeoning concept about retaining undiminished control over data in the cloud. For governments, ensuring data sovereignty has become a paramount concern (ENISA 2011, 40) which is calling for investigation into the notion, challenges and policies of data sovereignty.

Data sovereignty

The so much dreaded loss of sovereignty over data is a reflection of the initial finding that cloud computing is ***virtual***, ***dynamic*** and essentially ***stateless*** (NIST 2009). In a cloud environment information and the capacity it consumes are virtual assets and users' effective means of exercising control are greatly diminished. For example, users have to rely on the operator to locate where their information reside in the cloud but have no own means to establish its whereabouts (Petersen, Gondree and Beverly

[3] For example statutory compliance with the US Federal Information Security Management Act (FISMA), National Archives and Records Administration (NARA) and the General Services Administration (GSA).

[4] It is well beyond the scope of this paper to cover all possible security risks in a cloud environment which are discussed at length elsewhere (ENISA 2009; 2011).

2011, 1; Article 29 Data Protection Working Party 2010, 6). The dynamic nature of cloud services takes an additional toll on data sovereignty. Server capacity and computing cycles are used where it is cheapest (similar to least cost routing) and where there is spare capacity information is constantly passed around (Jaeger, Lin, and Grimes 2008, 276). Such optimization strategies, although perfectly legitimate from an economic point of view, render data hosting truly a moving target with unpredictable legal consequences. In addition, the same information is likely to be stored in multiple locations in order to back them up against losses and outages (Wyld 2009, 41). Finally, the statelessness should not be confused with lawlessness because cloud services are likely to transgress various jurisdictions. This globalization in turn triggers complicated dislocation where information stemming from one country is potentially exposed to one or several foreign jurisdictions. Operators of cloud computing services raise that they are "subject to divergent, and at times conflicting, rules governing jurisdiction over user content and data." (Microsoft Corporation 2010, 7)

What this concern means in practice can be best illustrated by looking at lawful interception, search and seizure authorities. In democratic countries the standard of protection against unreasonable searches is that law enforcement agencies have to obtain a search warrant before they can examine personal files stored on the harddrive of someone's computer (Nelson 2009, 10). However, in some jurisdictions, such as the US, cloud computing may be treated differently and the threshold of intervention can be significantly lower because the data has been handed over to a third party (Rayport and Heyward 2009, 37; West 2010b, 6; Wyld 2009, 43). As a result data residing on a cloud platform would be less protected than data on a personal harddrive or local servers.

If now a cloud service produces an additional crossborder effect the question arises: how many countries' local laws apply given that the physical establishment of the service provider, the country of origin of the user or of the data, and the actual data location could all be used as relevant criteria to establish jurisdiction? Intelligence services may enjoy even greater discretion to access data in the clouds due to these issues. The US PATRIOT Act is a notoriously cited example of a law which allows US government to request the disclosure of "any data stored in any datacenter, anywhere in the world if that system is operated by a US-based company." (Kushida, Murray, and Zysman 2011, 12) Most authors agree that such sweeping authorities can produce a deterrent effect for potential users of cloud services (Jaeger et al 2009; Kushida, Murray, and Zysman 2011, 12; Rayport and Heyward 2009, 38; Thibodeau 2011; Wyld 2009, 41).

Against this background the notion of data sovereignty unfolds which is in itself not limited to the cloud computing scenario, even though this is where the concern is

raised most prominently. In the literature to date no attempt to define data sovereignty has been made, and this section therefore sets out to develop a definition for the purpose of this paper. When Petersen, Gondree, and Beverly (2011, 1) refer to data sovereignty as the ability to "establish data location […] for placing it in the border of a particular nation state," this is mainly for the purpose of verifying and controlling the geo-location of data in the cloud. What is in the first place a condition for linking data to a jurisdiction this notion does not fully capture the essence of retaining sovereignty over data.

It also needs to be maintained that information are not protected as property as such. Depending on the circumstances intellectual property law, data protection law and laws protecting confidentiality and trade secrets may apply (Reed 2010, 1). Reed stresses that "the composite effect of these laws gives […] a level of control over its information which is very similar to owning physical property" (2010, 1). Information 'ownership', however, is a non-legalistic term commonly used to describe the relationship of somebody holding and administrating information on his or her own behalf. So understood it does not convey property rights.

As a point of departure sovereignty which is an established concept in philosophy and political science provides some initial insight. In spite of varying meanings throughout history, at its core it refers to supreme authority within a territory (Philpott 2010). Absolute sovereignty is composed of a positive and a negative meaning which only if taken together produces the desired effect. Its positive component could be circumscribed as the legitimate right to exercise authority which is matched by the negative component that no other authority could be legitimately invoked in this realm. In a next step this notion will be applied to data, which are intangible assets, and in relation to cloud services.

Contrary to national sovereignty data sovereignty describes a strategy to retain authority and control over digital information, for example through security measures. Apart from the ability to exercise full control over one's own data it entails that the data is not subject to any other authority that could demand access and retrieval. Already at this stage is becomes clear that data sovereignty is in practice rarely absolute because a state invokes authority over its subjects and their assets. Hence, individuals and private organizations can not enjoy full sovereignty over information but strive for authority and control within the boundaries of a given legal framework.

Only where the national authority is identical with the data owner (such as in the case of governments) one could conceive of absolute sovereignty, however, so far limited to the corresponding and exclusive jurisdiction. Negative sovereignty can be interfered with by malicious acts of cybercrime and is challenged whenever another jurisdiction lays claim on the data because it resides on the territory of a third state or

– as it is the case with the US PATRIOT Act - the cloud service provider is subject to rules that oblige it to hand over clients' data irrespective where it is stored (ENISA 2011, 40; West 2010b, 8). What government and other private users of international cloud services have in common is the risk of their data being exposed to the additional authority of yet another country. This cumulative effect appears to be a major shared concern.

The literature discussing the bearing of cloud computing on the right to privacy and the trade-offs of international data transfers develop a similar line of argument (Jaeger, Lin and Grimes 2008; Nelson 2009; Rayport and Heyward 2009). But it is important to note that in spite of significant overlaps with privacy and data protection concepts the notion of data sovereignty is wider because it is not limited to personal information only. Every digital snippet can be data and not everything is linked to an individual in such a way as it would be required for data protection laws to apply. Moreover, the potential uses and applications of cloud computing exceed personal data processing. For example business secrets, computing algorithms, mathematical modulations, physical simulations, and trade inventories or anonymized data is in need of a new paradigm when moved to and stored in the cloud. The rational for data sovereignty is not in the first place the protection of human dignity but something akin to the right to property and the right to the inviolable (digital) home. In a nutshell, what is missing in the information society is the comprehensive right to information ownership.

Far from being an established legal concept data sovereignty can be perceived as an information ownership claim which compensates for the progressing virtualization of information where digital data is stored and processed remotely. It covers therefore all legitimate expectations owners of all types of data entertain with respect to autonomy, control, security, privacy and the rule of law. These expectations may vary as does the legitimacy. For example lawful interception authority -- if well crafted and reasonably applied -- may be in conflict with the expectation of privacy but not legitimately so. It is not possible to determine the exact scope of data sovereignty regardless of the physical location of data and without a complete understanding of legal frameworks applying. Therefore, any definition in order to be meaningful would need to be set in its proper context. Using data sovereignty as a catchword like it is often done in contemporary public policy discourse may actually obfuscate more than contributing to an informed debate.

Turning now to governments cloud services above all, it should be recognized that governments have special considerations for which they want to retain sovereignty over public records and applications. Reasons are national security and defense, law enforcement, statutory duties of confidentiality, citizens' privacy protection, compliance with territoriality clauses in contracts and intellectual property rights etc.

In particular, governments resent the idea that any foreign power could exercise legitimate authority over their data (Kushida, Murray, and Zysman 2011, 12; Thibodeau 2011; Wyld 2009, 41). What distinguishes the public sector from the private sector is the ability to approximate absolute data sovereignty as long as exclusive jurisdiction over public data can be maintained. Hence, data sovereignty in the context of government data can be defined as:

> Government's control over all virtual public assets, which are not in the public domain, irrespective whether they are stored on own or third parties' facilities and premises, and which are governed under an effective information assurance framework, including, where appropriate, strategies to retain ***exclusive jurisdiction*** over government information.

For the purpose of this definition information assurance is the practice of managing ICT related risks in order to ensure confidentiality, integrity and availability.[5] It describes the set of rules and conditions for government to retain effective autonomy, security (covering confidentiality, integrity and availability), privacy and in appropriate cases exclusive jurisdiction over government data.

It is possible to address many of these requirements flowing from data sovereignty considerations with commercial offerings. The relationship with the cloud service provider are shaped via so called Service Level Agreements (SLAs) which stipulate the technical and legal obligations. Through procurement rules and with their bargaining power governments should be able to reach appropriate SLAs in particular concerning technical security. As a commercial agreement it does not, however, prevent third governments to invoke their authority. Because absolute sovereignty is not a commercial proposition governments set out to shape the conditions which guarantee undiminished sovereignty: Since sovereignty ties in with territoriality sensitive government information stay confined to national borders. This translates into a preference for national cloud services by governments which in many ways clashes with the global reach of cloud services.

Analysis of national cloud computing strategies

Depending on their electronic government maturity governments expand their existing strategies on the implementation of electronic government infrastructure to cloud computing strategies. Quite a number of countries have already drawn up or are in the process of devising their national cloud computing strategies for the public sector. This paper introduces and analyses comparatively the approaches to ensure

[5] Note that the Information Assurance concept can also cover five values, i.e. availability, integrity, authentication, confidentiality, and non-repudiation (Committee on National Security Systems (CNSS) 2010).

data sovereignty in cloud computing of – in this order -- the United States, the United Kingdom, Australia, and Canada. These four countries have been selected because of the progress made in adopting a strategy and their representative approaches with regards to protecting national data sovereignty.

United States

In 2009, the US Federal Government's Cloud Computing Initiative was announced (Kundra 2010, 2) followed by the release of the National Cloud Computing Strategy in 2011 (Kundra 2011). The central argument is that "for the Federal Government, cloud computing holds tremendous potential to deliver public value by increasing operational efficiency and responding faster to constituent needs." (Kundra 2011, 1) Migration to the cloud is with a potential target of 20 billion dollar one of the main budget items of federal IT expenditures which could eventually help save public money (1). In order to accelerate the pace of government take-up of cloud services the Federal CIO Council instituted a Cloud First policy which prescribes to explore first cloud service offerings before other new IT investments (2). The move towards cloud computing has to be viewed in the context with the initiative to consolidate federal data centers.

It is noteworthy that the NIST resumed the technical advisory role and contributes to definition and standard setting activities which essentially buttressed the federal approach[6] and are also an important point of reference for governments elsewhere (Danek 2010; ENISA 2011; Australian Government Department of Finance and Deregulation 2011).

The Federal Government is under the legal obligation to ensure security requirements such as compliance with the Federal Information Security Management Act (FISMA), agency specific policies pursuant to the Federal Information Processing Standards (FIPS) and many more rather fragmented and sometimes hard to comply with rules (WYLD 2009, 43).[7] Against this backdrop the Federal Cloud Computing Strategy explains the parameters for public organizations to consider when identifying their needs and planning cloud migration (Kundra 2011, 11f.). Value und readiness are the dimensions which determine an agency's roadmap. The strategy formulates a risk-based approach when determining what type of cloud service is appropriate (2011, 26). In other words it does not mandate the use of specific deployment solutions, such as a private cloud, but encourages to explore hybrid and community cloud offerings if they are adequate in addressing the associated risk level (or impact category).

[6] Corresponding to its statutory responsibilities for developing standards and guidelines under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

[7] FISMA defines three information security objectives, namely confidentiality, integrity and availability, and FIPS Publication 199 distinguishes three levels of potential impacts in the case of a security breach, *i.e.* low, medium and high impact (FIPS 2004).

Albeit data sovereignty is an explicitly acknowledged concern (2011, 30) it is not further explained how it will be treated. It can be assumed that it is considered as part of the risk management framework (2011, 26f.). However, many cloud service providers are US companies which may alleviate the problematic to some extent. West observes that agencies with high security needs generally require that information be stored in secure facilities within the continental US (2010b, 8). Government cloud services of the low-impact category could be in principle hosted in data centers abroad, however, some remain skeptical. Wyld comments that "[g]overnment at all levels has unique considerations, at the US federal, and certainly at the city and state and local level, we have concerns about the data residing within the US borders and not being at a cloud center somewhere around the world, […]" (The Brookings Institution 2010, 23).

United Kingdom

In 2009, the Digital Britain report was published which outlines the central policy commitments in the UK government's strategy to modernize the country and place it at the leading edge of the global digital economy. Reforming the public sector is one policy priority which covers broadly the further introduction and improvement of digital government as it is called in the report. Under the umbrella of efficient public sector procurement the vision of the G-Cloud is introduced which describes a dedicated cloud computing platform for sharing network-delivered services across government departments (UK Department for Business Innovation and Skills 2009, 212). The public cloud scenario, "where services can run on any server anywhere in the world," does not meet governmental needs for "data location, security, data recovery, availability and reliability." (213) It tasks the CIO Council to prepare the adoption of the G-Cloud as "a priority for government investments […] to secure efficiencies […] over the next three years." (UK Department for Business Innovation and Skills 2009, 213)

From the outset, the G-Cloud has been designed as a private government operated cloud infrastructure based on UK territory (UK Cabinet Office 2010a, 22; 2010b, 27). Besides, public cloud services co-exist and are already deployed by some public sector bodies, for example for services that do not process personal data (UK Cabinet Office 2010b, 4). Once constraints for UK's information assurance requirements can be addressed, including data centers being outside the UK, the use of public cloud service is expected to grow (4f.). For the time being G-Cloud private cloud services do already address these concerns and "enable earlier use of the shared utility model across the public sector" (5). A cloud first imperative requires the public sector to explore cloud service options before turning to other IT investments. The G-Cloud is accompanied by a data center consolidation strategy.

Australia

After a public consultation the Australian Government published its Cloud Computing Strategy in 2011. The adoption of government cloud services is appropriate "where they demonstrate value for money and adequate security" meeting the mandatory requirements outlined in the Protective Security Policy Framework (PSPF) (Australian Government Department of Finance and Deregulation 2011, 5). The strategy lists the need to be aware of data sovereignty requirements among the legal and regulatory risks (15). The need to be aware of legislative and regulatory requirements in other geographic regions is illustrated with the example of the US PATRIOT Act which is considered "a key concern for data stored in the cloud and located within the United States" (15). There is no prescription of the type of cloud services but decisions have to be based on a risk-managed approach which is taking into account information assurance requirements. Thus, low-risk services, such as government websites, could be run on a public cloud infrastructure. There are indications that apart from data sovereignty constraints regulations such as data protection laws and financial regulations may force domestic cloud services in some areas. The whole-of-government approach to cloud would be integrated with a data centre consolidation strategy.

Canada

Canada is trying to position itself as a suitable location for cloud infrastructure due to its cooler ambient climate, low population density, existing fibre networks and reliable power supply (Danek 2009). The Canadian government's cloud strategy is not well documented. In 2010, apparently the Government of Canada's cloud computing roadmap was endorsed (Danek 2010, 4). The approach to cloud computing rests on the NIST foundation and plans are to set-up the Government of Canada community cloud (9). The Canadian Policy on Management of Information Technology and the corresponding Government Security Policy endorse a security risk management approach which would also apply to the contracting of government cloud services.

Already in 2006, the Canadian Government issued a federal strategy to come to terms with the USA PATRIOT Act and transborder data flows (The Treasury Board of Canada Secretariat 2006). In order to protect the personal data of Canadian citizens the strategy advocates a risk-based approach to the protection of personal information. The policy document institutes as a rule that all outsourcing involving personal data has to be completed within Canada (22). It follows, that the Canadian Government would be confined to domestic cloud services whenever personal data of Canadian citizens is involved. As a means to establish control additional guidance for the contracting out of government information requires the agreement to be explicit about that the information is the property of the Government of Canada.

Comparative analysis of national data sovereignty strategies

The US and the UK form a pair of countries which are very ambitious in the scope, breadth and pace of their national cloud computing strategies. Australia and Canada are both on track and willing to adopt government cloud services but arguably with less agility. Ultimately, all countries' cloud computing strategies have been caught by concerns about the cloud's inherent data sovereignty problem. They consider data sovereignty a legal risk which can not be adequately addressed with technology or through contractual arrangements alone. The Australian and Canadian policies are outspoken about their constraint against authorities like the US PATRIOT Act. However, no country mandates across-the-board domestic cloud services although every country is selectively enforcing the territoriality paradigm.

All countries operate a mixed approach in which also public and cross-border government cloud scenarios are possible. All countries surveyed rely on risk management strategies in order to decide which cloud solution is adequate to meet a specific government need, for example pertaining to the security level. Risk assessments needs to comply with extensive government standards on IT security, also referred to as information assurance, in the course of which data sovereignty constraints come to play (*see* also ENISA 2009, 24). Yet, with different justifications each country has a certain disposition for keeping data within their national borders. In Australia and Canada data protection laws are a dominant factor in this regards. The UK's G-Cloud is specifically designed as a domestic facility. One could even argue whether the G-Cloud's architecture meets the definition of cloud computing concerning scalability. In the US's public sector arguably a preference for domestic cloud computing prevails.

If and how international law can contribute to create better conditions for international cloud computing and the extent to which this actually benefits data sovereignty is discussed in the last section below.

Multi-lateral regulation of cloud services

The pursuit of new international standards

When governments stress the international policy dimension of cloud computing and the unresolved policy issues coming with it they increasingly acknowledge the need for international standards (Australian Government Department of Finance and Deregulation 2011, 15; Kundra 2011, 30). For the US Federal Chief Information Officer Vivek Kundra data sovereignty is a legitimate challenge which cannot be addressed by technology alone: "It is going to be a question of international law, and treaties that we will need to engage in the coming years." (Kundra in Walker 2011) The legal uncertainties associated with international applications of cloud computing today are cited as one of the reasons why corporate users and the public sector

hesitate to fully embrace the new technology. The need for an international governance framework for cloud computing is compelling, however, it is very controversial how data sovereignty should be addressed in such a multi-lateral agreement. Initial proposals discussed at the World Economic Forum which call for the creation of a new universal body to oversee cloud computing are met with concerns that this will create inadequate regulation (WEF 2011, 16).

The prospects of a multi-lateral agreement which is not based on mutual trust are dim. Whether for data sovereignty it would be sufficient if countries under the rule of law ensure that national authority over data residing in the cloud adhere to due process requirements, especially requiring a warrant, and grant transparency is controversially discussed (Rayport and Heyward 2009, 49). It would certainly help to alleviate some of the constraints inhibiting governments and also the private sector if sweeping law enforcement authority is re-adjusted to internationally accepted levels.

It would be farfetched to believe that jurisdictions in cyberspace can be completely redefined in order to accommodate data sovereignty regardless where the data resides. Perhaps, it is even not desirable. The only real-world example in which sovereignty can take precedent over a given jurisdiction is actually the guarantee of diplomatic immunity which has a long tradition in international diplomacy and is codified in the Vienna Convention on Diplomatic Relations of 1961. The Convention grants diplomatic privileges and immunities for diplomats, to diplomatic missions and facilities, for diplomatic archives, documents, official correspondence and diplomatic bags, all of which are under certain conditions inviolable and declared immune from search, requisition, attachment or execution (Vienna Convention 1961, Articles 22f.).[8] This example, however, is much more suitable to illustrate the exceptionality of foreign sovereignty in a given jurisdiction and can not be regarded a viable solution to guarantee blanket sovereignty for every government information residing in the cloud.

However, it is not the first time that transborder data flows and its economic and political repercussions have been in the focus of an international public policy debate. Already in 1977, Louis Joinet, the then President of the French *Commission nationale de l'informatique et des Libertés*, observed that "the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows." (Joinet in Eger 1987) During the 1980ies international standard-setting activities pertaining to the protection of personal data while allowing for them to be transferred abroad took place. Notably, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereinafter OECD Privacy Guidelines, 1980) and the Council of Europe's Convention for the Protection

[8] This does not prevent covered intelligence gathering completely, *see* for example Spiegel Online International. "US Diplomats Told to Spy on Other Countries at United Nations". 28 November 2010.

of Individuals with regard to Automatic Processing of Personal Data (hereinafter Convention 108, 1981), have been devised with a view to create the conditions which would facilitate transborder flows of personal data (OECD 2010, 12).

As a means to this end both international instruments set forth common data processing standards for personal information which provide for a minimum of harmonization and thus, allow for data movement to other countries which comply with the same set of rules. Essentially, countries do not attempt to retain sovereignty over personal data from their citizens but are satisfied that receiving countries in which legal disputes would be adjudicated adhere to the data protection principles set out in the agreement. In this context the individual dimension of data sovereignty is foremost at stake because the consequences of a loss of sovereignty are mainly borne by the individuals to which the data belongs. Notably the cross-border enforcement of data protection laws has been a thorny issue and citizens from one country may find it difficult to exercise their rights in a third country to which their personal data has been transferred.

Ironically, what is deemed sufficient to protect citizens' personal data going abroad government do widely not perceive as adequate for the bulk of government information because data sovereignty is largely unresolved. Arguably, governmental users have different expectations on cloud services than the gross of the individual users for whom a change of jurisdiction and public authority does in most cases not matter as long as data protection regulation is complied with and the rule of law applies. In terms of sensitivity, however, personal information can be similar to many governmental data which should be an argument for ensuring a similar level of protection of data residing in the cloud. As a blueprint for an international governance framework for cloud computing existing international agreements on transborder flows of personal data cannot satisfy completely. Despite the harmonization from the common data protection standards national regulations greatly vary in detail and other national sectoral laws have to be taken account of. Moreover, the Convention 108 and OECD Privacy Guidelines do not resolve the problematic that transborder data flows can cause multiple jurisdictions adding-up which causes the much dreaded legal complexity.

What can be achieved, therefore, with a multi-lateral approach is to clarify who has jurisdiction over information during transit, while stored and processed, and efforts to avoid multiple jurisdictions as well as defining the minimum due process requirements for law enforcement surveillance, search and seizure of cloud infrastructure. When looking at the European Union the digital internal market with respect to cloud computing is still very much of an ideal, however, the available instruments to achieve further integration are explored below.

An European Union Digital Internal Market for Cloud Services

For the EU achieving an internal market for cloud computing would be a very worthwhile policy investment in the economic prospects and competitiveness of the region. In the Digital Agenda, a strategic policy paper, the European Commission recommends to develop “an EU-wide strategy on "cloud computing" notably for government and science” (European Commission 2010, 23). Neelie Kroes, the Commissioner responsible for the Digital Agenda, made it clear that the legal framework is part of the work for the envisaged cloud strategy focusing on an update of the EU data and privacy protection instruments and statutory user rights taking into account the international dimension of cloud technology (2011, 2). The Commission’s work in progress concerns other legal provisions as well that influence the deployment of cloud computing in public and private organizations (2011, 2). This outlook remains too vague to make a prognoses about the breadth and scope of the projected EU strategy but the language is reminiscent of economic integration through harmonization of national laws. This would not bring about a breakthrough on data sovereignty guarantees since the European Commission is more likely to develop their existing policy trajectories such as personal data and consumer protection.

Within its remit the so called Article 29 Working Party on Data Protection proposes to reduce the complexity stemming from multiple jurisdictions within the EU through strengthening the country of origin principle (Article 29 Working Party on Data Protection 2010, 31). Under this proposal the relevant criterion to determine applicable data protection law would be the location of the main establishment of the controller of the data, i.e. the person or entity which owns the data. The geo-location of data itself is irrelevant under the present data protection framework (8). What may help to simplify the otherwise conflicting application of data protection laws in a situation where several Member States are involved does not much to improve data sovereignty because of the limited scope of application and many overriding national competences.

Wyld prognoses a cooperation of Member States for an EU cloud infrastructure (2010, 8). An interesting utopian idea is promoted by the European Network and Information Security Agency (ENISA) which recommends “national governments and European Union institutions to further investigate the concept of a European Governmental cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied, both in terms of legislation and security policy and where interoperability and standardization could be fostered.” (2011, 9) The document does not elaborate further what this new cloud is about, and how it can be achieved. An supra national virtual space where authority is exercised under a common set of rules would be a way of guaranteeing data sovereignty acceptable to Member States. The establishment of a similar safe harbor knows no precedent and

participating nation states would be required to relinquish some of their sovereignty with an international agreement in order to gain data sovereignty. Whether such a proposal has any realistic chance to succeed depends on many factors but foremost how far countries are satisfied with their national strategies and if the European Union is willing to invest its sovereignty (*regime sui generis*) in such a project.

Conclusions

If cloud computing is the next paradigm in computing than governments can not miss this trend and continue to migrate public digital assets to cloud services. Governments find themselves in the dilemma to ensure sovereignty over data residing in the cloud which is virtual, dynamic and potentially stateless. Data sovereignty is an ideal conception of information ownership which compensates for the progressing virtualization of information where digital data is stored and processed remotely. For governments this means:

> Government's control over all virtual public assets, which are not in the public domain, irrespective whether they are stored on own or third parties' facilities and premises, and which are governed under an effective information assurance framework, including, where appropriate, strategies to retain ***exclusive jurisdiction*** over government information.

Countries treat this issue as a legal risk which can not be adequately addressed with technology or through contractual arrangements alone. Hence, in applying their national risk management strategy the countries surveyed (US, UK, Australia, and Canada) restrict cloud solutions for sensitive government information (medium- and high-risk) to their territory which contradicts the cloud technology's global philosophy.

The call for international policy to remedy the complexity of divergent, and at times conflicting, regulations of different countries pertaining to cloud computing can help to establish a viable commercial environment. International standard-setting may, however, not go far enough to provide a solution to governments' data sovereignty concerns over transborder flows of government data. From a risk-management point of view the territoriality paradigm which favors national cloud services would preempt any international agreement build on mutual trust.

Besides, the concept of data sovereignty offers a proposition how to strengthen the link between the data owner and the all types of data not limited to the protection of personal information. Cloud computing presents a scenario to argue that it is not

enough to update and harmonize existing regulation but to take information ownership rights to a new level.

References

Article 29 Data Protection Working Party. 2010. *Opinion 8/2010 on applicable law*. WP 179. Adopted on December 16. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf (accessed June 25, 2011).

Australian Government Department of Finance and Deregulation. 2011. "Cloud Computing Strategic Direction Paper". http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf (accessed June 25, 2011).

Booz Allen Hamilton. 2009. "The Economics of Cloud Computing. Addressing the Benefits of Infrastructure in the Cloud". http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf (accessed June 25, 2011).

Committee on National Security Systems (CNSS). 2010. *National Information Assurance (IA) Glossary*. CNSS Instruction No. 4009. April 26. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (accessed June 25, 2011).

Council of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108)*. Adopted in Strasbourg, 28. January 1981. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (accessed June 25, 2011).

Curtin, Gregory G. 2007. "E-Government". *The Encyclopedia of Political Communications*, Los Angeles: Sage Publications.

Danek, Jirka, CTO at Public Works Government Services Canada. 2009. *Cloud Computing ad the Canadian Environment*. October 6. http://www.scribd.com/doc/20818613/Cloud-Computing-and-the-Canadian-Environment#archive (accessed June 25, 2011).

Danek, Jirka, CTO at Public Works Government Services Canada. 2010. *Government of Canada (GC) Cloud Computing: Information Technology Shared Services (ITSS) Roadmap*. Presentation. http://isacc.ca/isacc/_doc/ArchivedPlenary/ISACC-10-43305.pdf (accessed June 25, 2011).

Eger, John M. 1978. “Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?” *Law and Policy in International Business* 10 (4): 1065-66.

ENISA. 2009a. *Cloud Computing. Benefits, Risks and Recommendation for Information Security*. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (accessed June 25, 2011).

ENISA. 2009b. *Cloud Computing Information Assurance Framework*. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework (accessed June 25, 2011).

ENISA. 2011. *Security & Resilience in Governmental Clouds*. http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport (accessed June 25, 2011).

European Commission. 2010. *A Digital Agenda for Europe*. COM(2010) 245 final/2. August 26. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF (accessed June 25, 2011).

Federal Information Processing Standards Application (FIPS). 2004. Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (accessed June 25, 2011).

Goldsmith, Stephen, and William D. Eggers. 2004. *Governing by Network: The New Shape of the Public Sector*, Washington: The Brookings Institution Press.

Jaeger, Paul T., Jimmy Lin and Justin M. Grimes. 2008. “Cloud Computing and Information Policy: Computing in a Policy Cloud?” *Journal of Information Technology and Politics* 5 (3): 269 - 283.

Jaeger, Paul T., Jimmy Lin, Justin M. Grimes, and Shannon N. Simmons. 2009. “Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing”. *First Monday* 14 (5-4). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171 (accessed June 25, 2011).

Kroes, Neelie, Vice-President of the European Commission responsible for the Digital Agenda. 2011. “Towards a European Cloud Computing Strategy”. Speech at the World Economic Forum, Davos, January 27. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50&format=PDF&aged=1&language=EN&guiLanguage=en (accessed June 25, 2011).

Kundra, Vivek (US Federal Chief Information Officer). 2010. “State of Public Sector Cloud Computing.” 20 May 2010. http://www.info.apps.gov/sites/default/files/StateOfCloudComputingReport-FINALv3_508.pdf (accessed June 25, 2011).

Kundra, Vivek (US Federal Chief Information Officer). 2011. *Federal Cloud Computing Strategy*. http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf (accessed June 25, 2011).

Kushida, Kenji E., Jonathan Murray and John Zysman. 2011. “Diffusing the Fog: Cloud Computing and Implications for Public Policy.” *BRIE Working Paper 197*. March 11, 2011. http://brie.berkeley.edu/publications/wp197.pdf (accessed June 25, 2011).

Mayer-Schönberger, Viktor, and David Lazer. 2007. “From Electronic Government to Information Government." In *Governance and Information Technology*, eds. Viktor Mayer-Schönberger and David Lazer. Cambridge, MA: MIT Press, 1-14.

McKinsey. 2009. “Clearing the Air on Cloud Computing.” (On file with the author).

Microsoft Corporation. 2010. “Building confidence in the cloud: A proposal for industry and government action to advance cloud computing.” http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/ConfidenceWP.doc (accessed June 25, 2011).

Nelson, Michael R. 2009. *Cloud Computing and Public Policy*. Briefing Paper for the ICCP Technology Foresight Forum, OECD. http://www.oecd.org/dataoecd/39/47/43933771.pdf (accessed June 25, 2011).

National Institute of Standards and Technology (NIST). 2009. "NIST Definition of Cloud Computing V15." http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf (accessed June 25, 2011).

OECD. 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Adopted on 23 September 1980.

http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html (accessed June 25, 2011).

OECD. 2010a. “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”. DSTI/ICCP/REG(2010)6/FINAL. *OECD Digital Economy Paper* 176. http://www.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/iccp/reg(2010)6/final&doclanguage=en (accessed June 25, 2011).

OECD. 2010b. *Greener and Smarter: ICTs, the environment and climate change*. Background report for the OECD Technology Foresight Forum on “Smart ICTs and Green Growth”, on 29 September 2010. http://www.oecd.org/dataoecd/27/12/45983022.pdf (accessed June 25, 2011).

Petersen, Zachary N. J., Mark Gondree and Robert Beverly. 2011. “A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud”. *Proceedings of HotCloud 2011*. http://znjp.com/papers/peterson-hotcloud11.pdf (accessed June 25, 2011).

Philpott, Dan. 2010. "Sovereignty", In *The Stanford Encyclopedia of Philosophy* (Summer 2010 Edition), ed. Edward N. Zalta. http://plato.stanford.edu/archives/sum2010/entries/sovereignty/ (accessed June 25, 2011).

Rayport, Jeffrey F., and Andrew Heyward. 2009. “Envisioning the Cloud: The Next Computing Paradigm”. A MarketspaceNext Point of View. http://marketspacenext.files.wordpress.com/2011/01/envisioning-the-cloud.pdf (accessed June 25, 2011).

Reed, Chris. 2010. “Information 'Ownership' in the Cloud.” Queen Mary School of Law Legal Studies Research Paper No. 45/2010. Available at SSRN: http://ssrn.com/abstract=1562461 (accessed June 25, 2011).

Robinson, Nail, Helen Rebecca Schindler, Jonathan Cave and Janice Petersen. 2010. *Cloud Computing in the public sector: rapid international stocktaking. Strategies and Impact.* http://www.scribd.com/doc/40866691/Cloud-Computing-in-the-Public-Sector (accessed June 25, 2011).

Spiegel Online International. 2010. “US Diplomats Told to Spy on Other Countries at United Nations”. November 28. http://www.spiegel.de/international/world/0,1518,731587,00.html (accessed June 25, 2011).

The Brookings Institution. 2010. "The Economic Gains of Cloud Computing". Washington, D.C. Wednesday, April 7. www.brookings.edu/events/2010/0407_cloud_computing.aspx (accessed June 25, 2011).

The Treasury Board of Canada Secretariat. 2006. *Privacy Matters. The Federal Strategy to Address Concerns About the USA PATRIOT Act and Transborder Data Flows*. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp-eng.pdf (accessed June 25, 2011).

Thibodeau, Patrick. 2011. "Congress Urged to Leave Cloud Computing Alone". *Computerworld*, April 12. http://www.computerworld.com/s/article/9215750/Congress_urged_to_leave_cloud_computing_alone_ (accessed June 25, 2011).

UK Cabinet Office. 2010a. *Government ICT Strategy. Smarter cheaper greener*. http://webarchive.nationalarchives.gov.uk/20100304104621/http://www.cabinetoffice.gov.uk/media/317444/ict_strategy4.pdf#page=23 (accessed June 25, 2011).

UK Cabinet Office. 2010b. *Data Center Strategy, G-Cloud, & Government Applictions Store Programme Phase 2*. http://www.cabinetoffice.gov.uk/sites/default/files/resources/01-G-CloudVision.pdf (accessed June 25, 2011).

UK Department for Business Innovation and Skills. 2009. *Digital Britain*. Final Report. http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf (accessed June 25, 2011).

Vienna Convention on Diplomatic Relations. 1961. United Nations Treaty Series, vol. 500: 95. http://untreaty.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf (accessed June 25, 2011).

Walker, Molly Bernhart. 2011. "Kundra: Cloud computing data sovereignty a matter for 'international law'", April 10. http://www.fiercegovernmentit.com/story/kundra-cloud-computing-data-sovereignty-matter-international-law/2011-04-10#ixzz1OmRYO9fI (accessed June 25, 2011).

West, Darrell M. 2010a. "Saving Money Through Cloud Computing." *Governance Studies at Brookings*. http://www.brookings.edu/~/media/Files/rc/papers/2010/0407_cloud_computing_west/0407_cloud_computing_west.pdf (accessed June 25, 2011).

West, Darrell M. 2010b. “Steps to Improve Cloud Computing in the Public Sector”. *Issues in Technology Innovation* 1, http://www.brookings.edu/~/media/Files/rc/papers/2010/0721_cloud_computing_west/0721_cloud_computing_west.pdf (accessed June 25, 2011).

World Economic Forum. 2011. *Advancing Cloud Computing: What To Do Now?* http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf (accessed June 25, 2011).

Wyld, David C. 2009. “Moving to the Cloud: An Introduction to Cloud Computing in Government”. *E-Government Series*. IBM Center for the Business of Government. http://www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf (accessed June 25, 2011).

Wyld, David C. 2010. “The Cloudy future of Government IT: Cloud Computing and the Public Sector Around the World”. *International Journal of Web and Semantic Technology* 1 (1), 1-20. http://airccse.org/journal/ijwest/papers/0101w1.pdf (accessed June 25, 2011)