Government Cloud Computing and National Data Sovereignty

Irion, K.

DOI
10.1002/poi3.10
Publication date
2012
Document Version
Final published version
Published in
Policy and Internet

Policy and Internet

Policy & Internet, Vol. 4, No. 3-4, 2012

Government Cloud Computing and National Data Sovereignty

Kristina Irion

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 for data sovereignty. This article explores data sovereignty in relation to government cloud services and how national strategies and international policy evolve. It concludes that data sovereignty presents national governments with a legal risk that cannot be adequately addressed with technology or through contractual arrangements alone. Governments therefore adopt strategies that aim to retain sovereignty over government information.

KEY WORDS: cloud computing, electronic government, data sovereignty, data ownership, information assurance, international data transfers, public policy

Introduction

Two major trends in information and communications technology (ICT) have come together in recent years: first, the public sector relies on electronic government solutions for its back-office operations. Electronic government describes the use of ICT in the public sector. Mayer-Schönberger and Lazer (2007, p. 4) state that "The 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." Second, cloud computing is fundamentally changing the way how computing is done by providing ubiquitous, on-demand access to computing resources. To governments cloud services hold the promise of rendering public service delivery and back-office operations more effective and efficient. Beyond the compelling cost economies that are expected to yield from the massive adoption of cloud services in the public sector, cloud technology is also a promising platform for open government, interagency cooperation, and government innovation. However, what looks like an ideal match actually raises a range of unresolved issues.

When "information is the foundation of all governing" (Mayer-Schönberger & Lazer, 2007, p. 1) then the modern treasury of public institutions is where the

Published by Wiley Periodicals, Inc., 350 Main Street, Malden, MA 02148, USA, and 9600 Garsington Road, Oxford, OX42 DQ.

wealth of public information is stored and processed. Government in most countries is under very strict obligations to ensure that public information technology (IT) systems and information are secure. Cloud services, however, are challenging in this regard because direct means of control over virtual assets are greatly diminished. Furthermore, national perspectives on how government data should be handled clash in many ways with the cloud's global philosophy as a service that transcends geographical and political boundaries (Kushida, Murray, & Zysman, 2011, p. 3). Thus, cloud services that are virtual and dynamic (National Institute of Standards and Technology [NIST], 2011a) take information governance to "a new level of abstraction" (Petersen, Gondree, & Beverly, 2011, p. 1).

Against this backdrop, many governments have raised concerns about national data sovereignty when government information is moved to the cloud. How can confidentiality of public information assets residing in the cloud be ensured? What if public information and IT systems are hosted abroad? Will government data of one country be caught under the authority of another jurisdiction? In the case of transnational cloud computing, does government data in the cloud's custody possibly affect national sovereignty? The notion of data sovereignty essentially seeks to compensate for the progressive virtualization of information by framing the government's quest for undiminished authority over government information assets. For the purposes of this article, national data sovereignty is defined here as:

> Government's exclusive authority and control over all virtual public assets, which are not in the public domain, irrespective whether they are stored on their own or third parties' facilities and premises.

This article explores national data sovereignty in relation to government cloud services and how national strategies and international policy evolve. It brings together the various strands of literature on electronic government, public policy of cloud computing, and of government cloud services. However, it does not attempt to investigate the wider landscape of technical security and data protection in government cloud services.

Public policy challenges of cloud computing have already attracted academic attention, mainly with regard 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, government surveillance, reliability, and liability. Nelson (2009) focuses on governments' role in fostering portability, competition, and innovation in cloud services. Reed (2010) discusses information "ownership" with respect to cloud services while acknowledging that property rights in information do not exist. Kushida et al. (2011) convey the core aspects of cloud computing service markets by looking at the influence policy issues have on their development. Since cloud computing is a burgeoning market and a marketing hype, corporations, analysts, and pundits discuss national and international policy issues

and address policymakers with varying sets of recommendations (Microsoft Corporation, 2010; Rayport & Heyward, 2009; World Economic Forum [WEF], 2011).

Public and private sector organizations seek to identify their data handling obligations in the realm of cloud computing. Pertinent issues that have been discussed in the literature include compliance with national laws on personal data protection and transborder data flows (e.g., Klein, 2008). The problematic of how and in what circumstances countries' lawful interception authority can be invoked to compel operators of cloud computing services to hand over clients' data residing in the cloud has also emerged as a distinct topic of inquiry. Walden (2011) offers a comprehensive discussion of law enforcement agencies' authority in the transnational environment presented by cloud computing. Law firms have issued briefings on this issue detailing legal aspects of transborder data transfers and the reach of lawful interception authorities (Linklaters, 2011; Noerr SNR Denton, 2011).

There are a handful of studies on government cloud services, mostly from the United States, that focus on the cost economies and challenges for governments' IT migration to cloud services. The most comprehensive study to date identifies 10 major challenges facing government in implementing cloud computing that are technical, regulatory, and organizational (Wyld, 2009). Paquette, Jaeger, and Wilson (2010) discuss cloud computing following a risk management approach in a governmental context. In one study, West (2010a) deals with cost economies from government cloud services in which he analyzes the available data. In a second study, he provides policy guidance to improve cloud computing in the public sector (West, 2010b). Robinson, Schindler, Cave, and Petersen (2010) offer an international overview of cloud computing in the public sector. 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. Data sovereignty is a notion that has been raised mainly in the context of government cloud services, but there has been no attempt to analyze this concept in the literature so far.

This article contributes to our understanding of the nature of sovereignty relating to virtual government data, a debate that has reopened with the advent of cloud computing. It argues that data sovereignty poses a pertinent public policy problem for governments everywhere, because it is a crucial dimension of national sovereignty that presupposes the nation state. After a discussion of the various lenses which can be used to view data sovereignty, the article investigates the implications of enforcement of data sovereignty in the context of government cloud computing. To this end, the cloud computing strategies of Australia, Canada, the United Kingdom, and the United States are introduced and analyzed with a view to safeguarding national data sovereignty. In spite of the early development, these countries have in common that they share a concern over national data sovereignty—even if the term is not used expressly in all cases—and they adopt a differentiated approach to come to terms with this challenge, typically involving limitations on the use of public cloud services to certain categories of government information, and geographical restrictions placed on certain government cloud

services. Finally, the article explores whether international agreements or European Union integration could address issues of sovereignty of government data in the cloud.

The article is structured as follows: the first section provides a concise introduction to cloud computing, followed by an overview of government cloud services and arguments. The next section turns to data sovereignty and how this concept is derived, followed by a comparative analysis of national cloud computing strategies of Australia, Canada, the United Kingdom, and the United States. The final section discusses the role of international policy and the European Union strategy for an internal digital market, and concludes.

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 et al., 2008, p. 271; Rayport & Heyward, 2009, pp. 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 desktop computer or a local server. Instead, applications and data are moved to shared data centers (Kushida et al., 2011, p. 4) in what technologists have dubbed "the cloud"—that is, 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 that owns and maintains the infrastructure also controls data and applications (Jaeger et al., 2008, p. 272). This positions cloud operators as a distinct type of Internet intermediary with their own eclectic range of policy challenges.

Cloud computing has emerged as a result of a number of technological advances, notably broadband connectivity; commodity server hardware with open interfaces; open source software for operating systems, web servers, and distributed computing; and open standards in Web 2.0 applications (Australian Government Department of Finance and Deregulation, 2011, p. 11; Nelson, 2009, p. 3; see also Armbrust et al., 2009, p. 6f). 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 et al., 2008, p. 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 have been central in the development of the cloud infrastructure, which infused interoperability and slashes the costs of software.

Various definitions of cloud computing are proposed in the literature, but the most widely cited is that NIST (2011a): "Cloud 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." This definition is composed of five characteristics: first, as an on-demand service, users can "unilaterally provision computing capabilities […] as needed automatically." Second, the cloud service can be accessed via broadband networks and standard protocols that support heterogeneous clients and user equipment. Third, resources are pooled to provision multiple users' demands with physical and virtual resources, for instance storage, processing, memory, network bandwidth, and virtual machines. Fourth, "capabilities can be rapidly and elastically provisioned" 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, based on which the utilized service is billable (NIST, 2011a).

Cloud computing "alters the basic economics of access to computing and storage" (Rayport & Heyward, 2009, p. 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 (Armbrust et al., 2009, p. 5f; Kushida et al., 2011, p. 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 economies of scale favor size. Kushida et al. (2011, p. 3) observe that "The 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." The flexible provision, the metered use, and the consumption-based pricing models have prompted comparisons to other utility services (Armbrust et al., 2009, p. 4; Jaeger et al., 2008, p. 271; Kushida et al., 2011, p. 4; Wyld, 2009, p. 56). Yet, the traditional concept of what a utility service is does not fit entirely, because cloud capacity is not simply a commodity but can be customized to support varying functionalities (Kushida et al., 2011, p. 4). Notwithstanding, it could develop into a 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 of today's popular Internet and Web 2.0 services 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 IT infrastructure and software, skip most in-house IT management and, instead, pay for exactly the computing capacity they utilize (Armbrust et al., 2009, p. 12f; Jaeger et al., 2008, p. 271f; Nelson, 2009, p. 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 their inherent transformative power are predicted to benefit society at large. Access to cloud technology releases new capabilities for innovation and entrepreneurship, and it facilitates market entry, scalability of operations, and experimentation (Kushida et al., 2011,

p. 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 (Nelson, 2009, p. 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 energy efficiency while bringing down overcapacities (OECD, 2010b, p. 22; Rayport & Heyward, 2009, p. 42).

Following the NIST taxonomy (NIST, 2011a), four different models of cloud computing are commonly deployed. The private cloud is an infrastructure which is operated exclusively for one client or organization and which is managed either by the organization itself or on its behalf by a third party.[1] A community cloud is a shared infrastructure with a common framework that supports a specific community managed by the organizations or a third party. 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, 2011a). Finally, the hybrid cloud combines two or more clouds (private, community, or public) that remain unique entities but that share some infrastructure, for example to balance the load between clouds. 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 is often kept on the premises. Further distinctions and assessment models can be used to describe various types of clouds under technical and commercial aspects[2]; however, for the purposes of this article it is sufficient to understand that from a technical point of view, cloud services are *virtual*, *dynamic*, and *without locational constraints*.[3]

Government Cloud Services

The substantial promise of cloud services meets the pronounced interest of many governments worldwide, who are conscious of how they spend taxpayer money and who are keen to find ways "to do more with less" (Wyld, 2009, p. 20). The public sector is very large, and sometimes even the biggest user of ICT in a given country; centralizing government's computational needs can leverage significant economies of scale. In most countries the public IT infrastructure, however, replicates government organization, with many dispersed data centers serving the needs of specific government departments. Additionally, server utilization has reportedly been low—sometimes as low as 7 percent—keeping generous contingencies, with the consequence that massive overcapacity is left unexploited (The Brookings Institution, 2010, pp. 3, 6). Government cloud services promise to overcome this fragmentation and to supersede the era of long-lived and decentrally managed IT projects. Cloud services can dramatically alter government procurement of computing cycles and software that can be bought as a commodity on a pay-as-you-go basis.

The most immediate objective of government cloud strategies is to increase the effectiveness and efficiency of administrative processes (Kundra, 2010, p. 9), and Wyld (2009, p. 10f) identifies governments' need to save public resources to be one of the main drivers of take-up of government cloud services. Analysts predicted, for the United States, that moving public sector operations to cloud services could eventually save from 65 to 85 percent of federal agencies' yearly IT budgets (Booz Allen Hamilton, 2009, p. 5). Although most estimates concur with the finding that government cloud services will curb public spending on IT services, the forecast savings vary considerably (West, 2010a, p. 2f). West (2010a, p. 3f) 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. On a cautionary note, a 2009 report disputed these cost savings for large entities altogether (McKinsey, 2009), maintaining that compared to large enterprise data centers, current cloud computing offerings are not per se more cost-effective. Some customized features of cloud services, 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 administration of IT systems is essentially out-sourced. For the public sector, which arguably has difficulty 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, p. 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, p. 4) asserts that developing countries can access the latest computing technologies via the cloud, provided they have an adequate Internet infrastructure available. Second, cloud computing further reduces the locational imperative in the organization of the public sector (Mayer-Schönberger & Lazer, 2007, p. 7), which could be transformed according to consideration of 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 Vivek Kundra, the former U.S. Chief Information Officer (CIO), it is the ideal platform for the movement of open data whereby the government democratizes its data and shares it with the public (The Brookings Institution, 2010, p. 14). 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 contribute to policy formulation. Note that in line with the prevalent electronic government discourse, a technology alone does not transform government (Mayer-Schönberger & Lazer, 2007, p. 4f), but it is up to the government to yield these results or, conversely, to confine the implementation of a technology to merely an efficiency-enhancing measure.

Cloud computing is also believed to set free innovative potential within government, "not as a magic wand for solving hard computing and managerial problems" (Nelson, 2009, p. 8) but by easing implementation of many computerized government operations as a result of enhancing efficiency. Once the collaborative features of cloud computing are fully realized, this new platform can foster cooperation and collaboration across government departments, which may form another source for innovation (Nelson, 2009, p. 8; Rayport & Heyward, 2009, p. 45). Mayer-Schönberger and Lazer (2007, p. 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, p. 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 & Eggers, 2004, p. 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 can embark on the use of 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, 2010, pp. 8, 38). In practice this is not trivial because consolidation may be resisted by government departments for 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 that need to be updated first (UK Department for Business Innovation and Skills, 2009, p. 211; West, 2010b, p. 5). For instance, Kundra highlights the costly replication of certification procedures in the United States where vendors have to "certify their solutions with hundreds of agencies" (The Brookings Institution, 2010, p. 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 et al., 2008, p. 274; WEF, 2011, p. 8; West, 2010b, p. 6). Security is a wide notion that includes all accidental or intentional incidents that 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, p. 6; Wyld, 2009, p. 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; see also ENISA, 2011, p. 83; Wyld, 2009, p. 36f). In fact, governments' security concerns often resonate with the loss of ownership of the physical storage medium and the resulting perception of diminishing control over public virtual assets in a

cloud computing environment where a third party operates the data centers. A part of this inhibition has become known as governments' quest for data sovereignty—an emerging concept about retaining undiminished control over data in the cloud. For governments, ensuring data sovereignty has become a paramount concern (ENISA, 2011, p. 40), in turn calling for the following investigation into the notion, challenges, and policies of data sovereignty.

Data Sovereignty

The much-dreaded loss of sovereignty over data is a reflection of the initial finding that cloud computing is a *virtual*, *dynamic* technology (NIST, 2011a) that operates *across borders*. In a cloud environment, information and the required processing capacity 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 resides in the cloud, and so far have no means to establish its whereabouts themselves (Article 29 Data Protection Working Party, 2010, p. 6; Petersen et al., 2011, p. 1). The dynamic nature of cloud services takes an additional toll on control over one's information: server capacity and computing cycles are used where it is cheapest (similar to least-cost routing) and where there is spare capacity; information is therefore constantly passed around (Jaeger et al., 2008, p. 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, p. 41).

As a result of the transnational environment, cloud services cross various jurisdictions (Kushida et al., 2011, p. 3). This globalization in turn triggers complicated dislocation where information stemming from one country is potentially exposed to one or several foreign jurisdictions. The question arising from transborder data transfers is not particularly new, but not less pervasive when cloud computing is the next computing paradigm: 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? Operators of cloud computing services object that they are "subject to divergent, and at times conflicting, rules governing jurisdiction over user content and data" (Microsoft Corporation, 2010, p. 7). Similar to other Internet intermediaries, the cloud service provider may be the point of entry for authorities to gain access to client data, which creates an additional liability to the confidentiality of data in the cloud's custody.

Jurisdictional Reach for Data in the Cloud's Custody

What this concern means in practice can best be illustrated by considering 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 someone's hard drive (Nelson, 2009, p. 10). However, in some jurisdictions, such as the United States, 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 & Heyward, 2009, p. 37; West, 2010b, p. 6; Wyld, 2009, p. 43). As a result, data residing on a cloud platform would be less protected than data on a personal hard drive or local servers. Moreover, intelligence services may enjoy even greater discretion to access data in the clouds.

It is important to carefully distinguish between two possible scenarios in which foreign jurisdictions might claim authority over data stored in the cloud: first, there is a cross-border effect because data originating from one country is transferred to another country. The outcome is straightforward in that under the receiving country's jurisdiction, powers can be invoked vis-à-vis the cloud service provider to require discovery of data in its custody. Second, there is no cross-border effect because the data does not leave the country of origin, yet the cloud provider can still be subject to a third country's law of discovery which takes extraterritorial reach. Finally, the cross-border scenario can occur in combination with the extraterritorial application of laws, rendering cloud service providers liable under multiple national laws and potentially forcing the disclosure of clients' data under particular circumstances.

The USA PATRIOT Act is a notoriously cited example of a law that allows the 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 et al., 2011, p. 12; also Noerr SNR Denton, 2011, p. 4). Its Section 505 is the legal basis for issuing National Security Letters (NSLs), which are subpoenas and that can require service providers to hand over transactional information about clients without a court order. NSLs cannot be used to access communications content or files of clients—to this end a court order according to Section 215 that amends the Foreign Intelligence Surveillance Act (FISA) can be issued from a special U.S. court that makes decisions in a secret procedure. For international jurisdiction of these powers it suffices that the company has minimal corporate contacts with the United States and is in possession, custody, or control over the data sought (Noerr SNR Denton, 2011, p. 3). In both NSL and Section 215 the request for data is commonly combined with a gag order preventing the organization from disclosing the existence of and compliance with the subpoena.

At this point it must be conceded that other countries' laws on interception do produce effects similar to the USA PATRIOT Act and are also governed by secrecy laws (Linklaters, 2011, p. 2ff, citing examples from Belgium, France, and Spain; Walden, 2011, p. 2). However, most authors would concur that such sweeping, and in particular extraterritorial, powers can produce a deterrent effect for potential users of cloud services (Jaeger, Lin, Grimes, & Simmons, 2009; Kushida et al., 2011, p. 12; Rayport & Heyward, 2009, p. 38; Thibodeau, 2011; Wyld, 2009, p. 41). What manifests as a lack of trust is the prevailing lack of transparency, insufficient safeguards, the transnational setting, and resulting legal

complexity, none of which help to ascertain what happens to data in the cloud's custody and what the legal consequences for the data controller are.

Framing Sovereignty Over Data

Against this background the notion of data sovereignty takes shape, which is not an established legal concept but simply shorthand for retention of authority and control over information assets. As with many new and emerging concepts, data sovereignty is used to mean different things in various contexts. Notably in relation to cloud services, data sovereignty surfaced most prominently in policy discourse (Australian Government Department of Finance and Deregulation, 2011, p. 15; Gartner Research, 2011; Kundra, 2011, p. 30; Thibodeau, 2011; WEF, 2011, p. 11); however, it has a potentially much wider field of application. This section therefore sets out to frame sovereignty over data for the purpose of this article. To this end it explores institutions, expectations, and processes, which are central to this notion.

Information and data are intangible assets. Contrary to legal claims over tangibles, sovereignty over data cannot be founded on property rights. Property rights subsist in chattels that data may be recorded on—such as sheets of paper, pen drives, or servers—but not in information itself. Depending on the circumstances, intellectual property law, data protection law, and laws protecting confidentiality and trade secrets may apply; however, there is no corresponding legal basis to the widespread perception of property and ownership over digital information on the part of ICT users (Reed, 2010, p. 1). Information "ownership" is a nonlegalistic term commonly used to mean that information "belongs" to an individual user or organization who administers this information on their own behalf. Thus, data sovereignty cannot be derived from property rights.

Despite significant overlaps, information privacy and data protection do not provide a legal basis for data sovereignty, which is conceptually broader. Personal information is the protected subject matter of all data protection regulations. However, every digital snippet can be data, and it is not always linked to an individual in such a way as would be required for data protection laws to apply. For example business secrets, computing algorithms, mathematical modulations, physical simulations, trade inventories, or anonymized data are in need of a new paradigm, especially when kept off-premise for remote computing. Moreover, the rationale for data sovereignty is not in the first place the protection of human dignity, but something akin to the right to the inviolable (digital) home. Data sovereignty can thus be perceived as a gap-filling claim for authority and control over information assets, which would compensate for the progressive disenfranchisement from virtualization in data processing. In a nutshell, what is missing is a general principle in information governance that helps to uniquely attribute digital information and to confer control to this person or organization.

Originating from IT management parlance, data sovereignty has evolved into one of the most pertinent information governance issues today. Owing to this origin, the concept draws on information assurance approaches, that is, the practice

of managing IT-related risks in order to ensure confidentiality, integrity, and availability.[5] Information assurance is a process-driven approach to systematically address threats and vulnerabilities to information and information systems. The process follows through a set of assessments in which the information is first classified according to impact levels, and then followed by the actual risk assessment, which in a last step is used to define information assurance requirements that are commensurate to these risks. For example, the 2009 reports of the European Network and Information Security Agency (ENISA, 2009a, 2009b) present a widely recognized information assurance approach to cloud computing, the aim being to approximate data sovereignty at the individual and organizational level through technical and organizational requirements. Insofar, data sovereignty is not more than a new label for an existing information management practice.

The relationship between the service provider and the user of cloud services is formalized with a private contract that defines the obligations and rights, respectively. The terms and conditions of such contracts vary depending on whether it is a standard or a customized offer, which is likely to affect the level of responsibility the cloud service provider assumes (Bradshaw, Millard, & Walden, 2011, p. 188). The contract binds the parties to so-called service-level agreements (SLAs) typically stipulating the technical and legal obligations of the cloud service provider, including what has been agreed as information assurance requirements. It is possible to address many of the information assurance requirements flowing from data sovereignty considerations with commercial offerings. Data sovereignty in its entirety, however, cannot be a commercial proposition for two reasons. First, a private contract is only binding between its parties and does not confer a legal status beyond this scope. Second, cloud service providers must meet legal obligations under the jurisdictions they are subject to, for example, complying with data disclosure authority. With some variations this is also acknowledged as a standard reservation of the service provider to this type of contract (Bradshaw et al., 2011, p. 205f).

When Petersen et al. (2011, p. 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. It is, however, a condition for linking data to a jurisdiction, inasmuch as it is not possible to determine the exact scope of data sovereignty without knowledge of the physical location of data, and without a complete understanding of legal frameworks applying. Therefore, any attempts to assess the actual risks for data sovereignty would need to be set in their proper context.

What makes the idea of data sovereignty contentious in contemporary national and international policy dialog links back to transnational problems of jurisdiction over information assets.[6] It neatly reflects concerns about cloud computing where information is handed over to the custody of a cloud service provider without the legal certainty of which, and how many, national legal regimes could invoke their authority. This cumulative effect and the additional possibility to access data via the service provider appear to be the major shared concerns (Gartner Research, 2011). Bradshaw et al. (2011, p. 206) mention the

jurisdictional dislocation of data as one of today's key legal concerns. Correspondingly, information assurance processes adapted to cloud computing include both jurisdictions and foreign law as legal risks that need clarifying (ENISA, 2009b, p. 24; 2011, p. 40).

At present, concerns over data sovereignty may be overstated in relation to the actual risk of, for example, forced disclosure (Gartner Research, 2011). This is also exploited as a ready smokescreen behind which cloud service providers attempt to protect their local interest against foreign competition (Reding, 2011b). Policymakers and industry expect that a more nuanced understanding of data sovereignty will develop over the coming years as user confidence in cloud technology grows and industry-wide standards for cloud computing provide an acceptable reference framework. Still, the concern is unlikely to completely disappear (Gartner Research, 2011), and data sovereignty has the potential to bundle wider information "ownership" considerations. Governments and public sector bodies are by all means special customers of cloud technology, with distinct needs and requirements in this regard. The following section explores their stance and offers a definition of data sovereignty for the purpose of government cloud services.

National Data Sovereignty

Governments have special considerations for which they would seek sovereignty over public records, government information, and applications. Reasons include national security and defense, law enforcement, statutory duties of confidentiality, citizens' and public employees' privacy protection, and compliance with territoriality clauses in contracts and intellectual property rights, etc. On these grounds governments in most countries are under very strict obligations to ensure that public IT systems and information are secure. As a matter of legacy, existing regulations on public sector information assurance often predate the era of cloud computing (e.g., for the United States, see Paquette et al., 2010, p. 250) and take it for granted that data is stored in a government-controlled facility or is outsourced to a dedicated service provider. Although this forms a major impediment to government cloud computing, it is a transitory one.[7] Above all, cloud technology poses more fundamental challenges to the public sector compared to traditional IT management because it takes information governance to a new level of abstraction (Petersen et al., 2011, p. 1).

Depending on their electronic government maturity, many governments are in the process of developing an information governance approach, which would extrapolate public sector information assurance for the purpose of cloud computing. They find themselves in a difficult, almost Catch 22, situation: given the prevailing uncertainties over standards, policies, and legal issues, Paquette et al. (2010, p. 251) put deliberate planning and technical proficiency first, which would delay the swift adoption of cloud technology by the public sector. Yet, besides the compelling cost economies, many public and private stakeholders expect governments to raise the overall market acceptance of cloud technology in their countries by migrating some public sector operations to the cloud. By

leveraging their bargaining power, governments can give the necessary impetus to the development of sector-wide information governance approaches that would address the many risks associated with cloud computing. These processes inevitably raise the issue of national data sovereignty.

As a point of departure, the concept of sovereignty established in the social sciences is used to query its relevance for government information assets. Despite varying meanings throughout history, at its core sovereignty refers to supreme authority within a territory and over its population (Philpott, 2010; Weber, 1978). Sovereignty is composed of an internal and an external dimension, which only if taken together produce the desired effect. Internal sovereignty means that a state enjoys a monopoly of the legitimate right to exercise authority within a given territory. External sovereignty presupposes that no other authority could be legitimately invoked in this realm. The principle of mutual exclusion is the essence of external sovereignty and "it is this principle that defines territoriality in the international system" (Reinicke, 1998, p. 58). Without exception, digital information is subject to the sovereignty of the country in which it resides, and thus the territoriality paradigm extends to the virtual sphere. As discussed earlier, in the context of cloud computing a country's sovereignty can be contested. Reasons for this include the fact that the same digital information can be stored at various geographical locations spanning different countries, in addition to issues regarding the reach of extraterritorial legislation.

In turn, the effective exercise of national authority rests on the public sector information that "is the foundation of all governing" (Mayer-Schönberger & Lazer, 2007, p. 1). After all, public sector information embodies the past, the present, and the future of a country. The ability to govern presupposes command and control over government information to the extent necessary to deliver public services and public goods as well as to ensure the integrity of the state. One could even assert that national sovereignty is conditional upon adequate data sovereignty.[8] If a country has no effective means of controlling public information it will become in parts dysfunctional. If crucial information were controlled by a foreign power the country would be a colony. All countries therefore insist on unconditional sovereignty over government information that is for various reasons confidential, mission-critical, or sensitive to the functioning of the state. In particular, governments resent the idea that any foreign power could exercise legitimate authority over their data (Bradshaw et al., 2011, p. 198; Kushida et al., 2011, p. 12; Thibodeau, 2011; Wyld, 2009, p. 41). Governments are therefore likely to adopt strategies in pursuit of data sovereignty.

Since national sovereignty ties in with territoriality, special categories of government information can be expected to stay confined to national borders with the aim of avoiding foreign law. This would translate into a preference for national cloud services by governments, which in many ways clashes with the global reach of cloud technology. In attempting to shield special categories of government information from the extraterritorial reach of foreign disclosure laws, some governments consider including as a procurement requirement that the service provider is not under any obligation of data disclosure and under no

circumstances transfers government data without government consent.[9] If practiced, such a provision could effectively lead to the exclusion of service providers from countries that mandate extraterritorial data disclosure from public procurement for cloud services. Against this backdrop, the next section analyzes selected national cloud computing strategies, as well as related public sector regulations and their bearing on national data sovereignty.

Analysis of National Cloud Computing Strategies

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 article introduces and analyzes comparatively the approaches to ensure data sovereignty in cloud computing of 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 regard to protecting national data sovereignty.

The United States

The U.S. Federal Government's Cloud Computing Initiative was announced in 2009 (Kundra, 2010, p. 2), followed in 2011 by the release of the National Cloud Computing Strategy (Kundra, 2011). The strategy's 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, p. 1). With a potential target of 20 billion dollars, migration to the cloud is one of the main budget items of federal IT expenditure, which could eventually help save public money (Kundra, 2011). The move toward cloud computing has to be viewed in the context of the initiative to consolidate federal data centers. NIST assumed a technical advisory role and contributes to definition and standard-setting activities which essentially buttress the federal approach,[10] and are also important points of reference for governments elsewhere, such as Australia, Canada, and the United Kingdom (Australian Government Department of Finance and Deregulation, 2011; Danek, 2010; ENISA, 2011; UK Cabinet Office, 2011, p. 3).

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, p. 43).[11] Since these federal regulations pre-date cloud computing there is little certainty whether compliance is at all possible (Paquette et al., 2010, p. 260). In late 2011, NIST issued a draft Government Cloud Computing Technology Roadmap, which offers recommendations for government-wide implementation of cloud computing solutions. Once adopted, these recommendations will be particularly relevant for industry since they require some harmonization of cloud computing offerings. The Federal Risk

and Authorization Management Program (FedRAMP)[12] was established to bundle security certification procedures for cloud computing providers and reuse assessments and authorizations.

The Federal Cloud Computing Strategy explains the parameters that public organizations should consider when identifying their needs and planning cloud migration (Kundra, 2011, p. 11f). Value of, and readiness for, cloud migration are the dimensions that determine an agency's roadmap. The National Cloud Computing Strategy formulates a risk-based approach when determining what type of cloud service is appropriate (Kundra, 2011, p. 26). In other words, it does not mandate the use of specific deployment solutions, such as a private cloud, but encourages the exploration of hybrid and community cloud offerings if they are adequate in addressing the associated risk level (or impact category). In order to accelerate the pace of government take-up of cloud services, the Federal CIO Council instituted a Cloud First policy, which prescribes exploration of cloud service offerings before any new IT investments (Kundra, 2011, p. 2). Federal agencies are required to migrate three applications to the cloud by June 2012.

The General Service Administration (GSA), a branch of the U.S. Federal Government in charge of public procurement, among other things, announced that it will use Blanket Purchase Agreements (BPAs), which is to become the federal government's main cloud computing acquisition mode. The BPA is a framework contract through which government and public bodies at various levels can easily provision themselves with government cloud services from a government application store.[13] The GSA's first BPA for public cloud services lists as a requirement for vendors that all services acquired under the BPA must reside in continental U.S. territory (US GSA, 2011, p. 7). This BPA concerns public cloud services of the category Infrastructure as a Service (IaaS), corresponding to the FISMA moderate impact data security level. A second request for quotation for email as a service allows a separate quotation for both U.S. and non-U.S. hosted services, where the ultimate choice would then be left to the public body which is making a purchase decision.[14] The GSA justifies the data center location requirements with the security needs of federal agencies, and that the transfer of U.S. federal data abroad raises a variety of concerns "including the potential of foreign jurisdictions to assert access rights" (US Government Accountability Office [GAO], 2011, p. 4f).

National data sovereignty is an explicitly acknowledged concern (Kundra, 2011, p. 30), which evidently affects federal public procurement. However, many cloud service providers are U.S. companies, which may alleviate the problem to some extent. West (2010b, p. 8) observes that agencies with high security needs generally require that information be stored in secure facilities within the continental United States. Government cloud services of the low-impact category could in principle be hosted in data centers abroad; however, some government officials remain skeptical. Wyld comments that "Government at all levels has unique considerations, at the United States federal, and certainly at the city and state and local level, we have concerns about the data residing within the United States' borders and not being at a cloud center somewhere around the world" (The Brookings Institution, 2010, p. 23).

The United Kingdom

The Digital Britain report was published in 2009, outlining the central policy commitments in the U.K. government's strategy to modernize the country and place it at the leading edge of the global digital economy (UK Department for Business Innovation and Skills, 2009). Reforming the public sector is one policy priority that broadly covers 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. In its original version the G-Cloud is described as a dedicated cloud computing platform for sharing network-delivered services across government departments (UK Department for Business Innovation and Skills, 2009, p. 212). Hereafter, 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" (UK Department for Business Innovation and Skills, 2009, p. 213).

The 2011 Government Cloud Strategy, however, shows a significant emphasis shift when stating that the "Government cloud is not a single, government owned, entity; it is an ongoing and iterative programme of work which will enable the use of a range of cloud services" (UK Cabinet Office, 2011, p. 5). Thus, the original plans to operate a private government cloud were abandoned for a more flexible public cloud first policy, except in some areas where secure private cloud provision is imperative (UK Cabinet Office, 2011, p. 5). What has been inspired by the U.S. cloud strategy entails another paradigm shift in public sector IT culture: "The move from custom to commodity solutions" (UK Cabinet Office, 2011, p. 7). As such the G-Cloud program introduces cloud services and commodity ICT in government (UK Cabinet Office, 2011, p. 15). Quoting Liam Maxwell, the Cabinet Office's director of ICT futures, self-provisioning of IT services by authorities should become as easy as buying stationery (Best, 2012). As is the case for the United States, the G-Cloud is accompanied by a data center consolidation strategy.

The revamped G-Cloud strategy announces a pragmatic and consolidated application of public information assurance requirements. Under a new information assurance governance arrangement, once core and commodity IT services pass assurance and accreditation they receive blanket certification (UK Cabinet Office, 2011, p. 13f). The strategy holds that at any given time, cloud service providers may be required to report the particular legal and regulatory frameworks that apply to government information in their custody (UK Cabinet Office, 2011). This strategy itself does not impose geographic limitations on public cloud services. In order to understand what categories of government information assets can be internationally sourced and what information assurance requirements have to be met, the G-Cloud strategy must be read in conjunction with the guidance on ICT off-shoring (UK CIO Council, 2011). According to this guidance, government data with national security protective markings should not be processed outside of the United Kingdom if being exposed to third country administrations' control or influence (UK CIO Council, 2011).

Early 2012 saw the first tender for government cloud services.[15] Suppliers need to pass assurance and accreditation in order for their services to be listed in the G-Cloud catalogue, that is, the government application store from which public sector buyers can provision themselves with a whole range of cloud services. In principle, the tender and the accreditation would permit government information assets up to moderate impact levels to sit in public clouds; however, only government information assets up to low impact levels can be off-shored (i.e., outside the European economic area; UK CIO Council, 2011, p. 3) and under the framework contract suppliers are prohibited from complying with any data disclosure requests without the consent of the government.

Australia

The Australian Government published its Cloud Computing Strategy in 2011, after a public consultation. According to this strategy, 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 (Australian Government Department of Finance and Deregulation, 2011, p. 5). The strategy lists the need to be aware of data sovereignty requirements among the legal and regulatory risks (Australian Government Department of Finance and Deregulation, 2011, p. 15). The need to be aware of legislative and regulatory requirements in other geographic regions is illustrated with the example of the USA PATRIOT Act, which is considered "a key concern for data stored in the cloud and located within the United States" (Australian Government Department of Finance and Deregulation, 2011, p. 15). There is no prescription of the type of cloud services, such as public or private cloud offerings, but decisions have to be based on a risk-managed approach, which takes into account information assurance requirements. Thus, nonsensitive information, such as government public websites, could be run on a public cloud infrastructure (Australian Government Department of Finance and Deregulation, 2011, p. 20). The whole-of-government approach to cloud services would be integrated with a data center consolidation strategy. In late 2011, the Australian Government consulted with the public on a range of Cloud Better Practice Guides covering privacy, negotiation, and financial issues. Notably, implications from Australian privacy laws and transborder data flows trigger measures to ensure national data sovereignty. At present, there is no central public procurement activity with regard to government cloud services.

Canada

The Public Works and Government Services Canada (PWGSC) is the central government unit in charge of organizing information management and IT on behalf of federal government departments and agencies. PWGSC implements the Government of Canada IT Shared Services strategy, which has as its goal the more effective management of IT resources, the avoidance of duplication, and

the more efficient and cost-effective delivery of public services. The Canadian Policy on Management of Information Technology and the corresponding Government Security Policy endorse a security risk management approach that binds government internal and outsourced IT services.

The official cloud computing roadmap and a governance framework were endorsed in 2010, which led to the setting up of the Government of Canada's Community Cloud (the "GC Community Cloud"; Danek, 2010, pp. 4, 9). The PWGSC IT Service Branch offers various cloud-based IT services to federal government units that are located at the GC Community Cloud. The GC Community Cloud and the services it operates will be certified in line with the security architecture required for government-wide shared IT services (PWGSC/ITSB/CTO, 2011). The same security standards would apply to a public cloud provider under contract to the Government of Canada; however, guidance on the public procurement of cloud services has not yet been issued.

It must be noted that federal and provincial privacy regulations are another complex set of laws that must be observed by public sector bodies in relation to public cloud services. For reasons that combine privacy with data sovereignty concerns, the exposure of Canadian citizens' data to the laws of foreign jurisdictions has received much attention locally (Klein, 2008; The Treasury Board of Canada Secretariat, 2006, 2010). For example, in three Canadian provinces data protection laws for the public sector require special consideration in the event of public procurement that would expose personal information to the laws of foreign jurisdictions (see Klein, 2008, p. 11).[16]

Finally, Canada is positioning itself as a suitable location for cloud infrastructure due to its cooler climate, low population density, existing fiber networks, and reliable power supply (Danek, 2009).

Comparative Analysis of National Data Sovereignty Strategies

The following comparison between the state of government cloud computing in the United States, the United Kingdom, Australia, and Canada seeks to clarify if and how data sovereignty manifests itself in the domestic approach, and also to distinguish data sovereignty from other causes that may restrict a government's take-up of cloud services. Despite the different pace of development in the four countries, government cloud services form part of a wider effort to increase the sharing of IT resources across government departments, mainly with the efficiency-enhancing objective of consolidating and restructuring the operations of government data centers. The United States and the United Kingdom form a pair of countries that are very ambitious in the scope, breadth, and pace of their national cloud computing strategies. Both countries see cloud computing as an opportunity to change the way government procures ICT. Both Australia and Canada are on track and willing to adopt government cloud services, but to different conditions and at their own pace.

Australia, Canada, and the United Kingdom—like the United States—build their national cloud strategies on the NIST cloud definition (NIST, 2011a). Beyond

the basic definition of what comprises a cloud service, governments' cloud computing strategies differ significantly. The first important differentiation is whether a country decides to operate primarily a community cloud (e.g., Canada), or to rely to a substantial degree on public cloud services (e.g., the United States, and recently the United Kingdom). A government-operated community cloud is likely a domestic infrastructure, but this does not preclude the possibility for additional public cloud scenarios where appropriate. Where government's preference is set on public cloud services it could selectively enforce geographic restrictions which—it must be recalled—are not a feature of cloud technology.

National data sovereignty is the main rationale that explains geographic restrictions with legal risks of transborder transfers of government information, because these cannot be adequately addressed with technology or through contractual arrangements. The Australian policy includes constraints against foreign disclosure authorities. The United Kingdom has a clear policy on IT offshoring that limits cloud solutions for government (UK CIO Council, 2011, p. 8). The U.S. GSA considers foreign jurisdictions that could assert access rights over government data as a major impediment for federal agencies to accept cross-border cloud services (see Note 14). Finally, Canada is known to take a prudent approach to cross-border data transfers, as evidenced by IT outsourcing projects with an impact on citizens' personal data protection (The Treasury Board of Canada Secretariat, 2006, 2010).

The interplay of policies and processes relevant to government cloud computing is highly distinct for each country. At the most general level, data sovereignty bears relation to government policies on information handling and corresponding information assurance policies. The concept then surfaces at various stages in the adoption process as a requirement in public procurement, and finally in the security accreditation of service providers. Risk management strategies can be geared to cloud computing and to a certain extent be standardized for specific categories of cloud services (ENISA, 2011; NIST, 2011b). At present, NIST in the United States has put together the most advanced and conclusive information governance framework for cloud computing (NIST, 2011b). In the United States, the United Kingdom, and Canada, central security certification (or security accreditation) of cloud service providers is about to be introduced, which bundles and implements cloud security requirements by the government.

Information assurance procedures prescribe that risks for the confidentiality, integrity, and availability of information and information systems are classified in impact levels. National classification systems vary, for example, zero, low, moderate, and high, but, for example, the United Kingdom introduces further granularity. In principle, legal risks for national data sovereignty apply for any impact category, but special requirements are triggered as a result of certain impact levels. For example, at one extreme, government information of the high-risk category would be disqualified from being sent to public cloud services and transborder processing. At the other extreme, where there is no risk, such as in the case of public information on government websites, no special requirements

Table 1. Government Use of Public Cloud Services

United States: GSA Blanket Purchase Agreement							
Impact Level	Zero			Low	Moderate		High
Policy	BPA for moderate impact level is certainly downward compatible				BPA for IaaS Public cloud restricted to continental US territory BPA for SaaS E-mail Separate quotation for either US or non-US hosted services		Not tendered
United Kingdom: G-Cloud Framework (IaaS, PaaS, and SaaS)							
Impact Level	0—None	1—Minimal	2—Protect	3—Restricted	4—Confidential	5—Secret	6—Top Secret
Policy	Off-shoring possible Government consent for information disclosure			Restricted to EEA Government consent for information disclosure	Not tendered No off-shoring outside UK (UK CIO Council, 2011, p. 8)		

Note: BPA, Blanket Purchase Agreement; IaaS, Infrastructure as a Service; EEA, European Economic Area; PaaS, Platform as a Service; GSA, General Service Administration; SaaS, Software as a Service.

are needed. However, since the actual risk assessments are not published, it can be difficult to explain the rationale for geographic restrictions placed on providers of public cloud services.

Table 1 summarizes the gradual protection of national data sovereignty in the United States and the United Kingdom where government cloud services are already procured. In both countries government procurement of cloud computing has been centralized and structured in two main phases. In the first phase, service providers are selected and have to pass security accreditation or certification. In the second phase, government units and public bodies can provision themselves with cloud services on the basis of a prenegotiated framework agreement from a government application store. In practice, the United States and the United Kingdom allow for geographical restrictions at moderate impact levels and do not tender cloud services above a moderate impact level.

Ultimately, all countries' cloud computing strategies are affected by concerns about the cloud's inherent data sovereignty problem. It is arguably difficult to pin down when data sovereignty considerations have motivated a government decision to refrain from public and/or transborder cloud services. The tenets of information assurance, security, information "ownership," data protection,[17] and legal risks operate as facets of sovereignty over data. Eventually, the newly emerging centralization in public procurement and accreditation of cloud services drives standardization also with regard to safeguards for national data sovereignty. Because national data sovereignty is not merely a transitory phenomenon, geographical zoning of public cloud services is bound to persist; however, the extent of this will depend on the ability to develop an appropriate international information governance framework.

Multilateral Regulation of (Government) Cloud Services

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, p. 15; Kundra, 2011, p. 30). For the former U.S. CIO, Vivek Kundra, data sovereignty is a legitimate challenge: "It is going to be a question of international law, and treaties that we will need to engage in the coming years" (Walker, 2011). This section explores various avenues for the multilateral regulation of cloud services by analogy with the guarantee of diplomatic immunity, transborder data flows and data protection frameworks, and interstate mutual assistance procedures, before looking at the potential for a European Union digital internal market for cloud services.

Exceptional Guarantee of Diplomatic Immunity

It would be farfetched to believe that jurisdictions in cyberspace can be completely redefined in order to accommodate data sovereignty regardless of where the data resides. It is perhaps not even desirable. The only real-world

example in which sovereignty can take precedence over a given jurisdiction is the guarantee of diplomatic immunity codified in the Vienna Convention on Diplomatic Relations of 1961, which has a long tradition in international diplomacy. The Convention grants diplomatic privileges and immunities for diplomats, for 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).[18] This example, however, is much more suitable to illustrate the exceptionality of foreign sovereignty in a given jurisdiction and cannot be regarded as a viable solution to guarantee blanket sovereignty for all government information residing in the cloud.

Transborder Data Flows and Data Protection

The issues surrounding cloud services are not the first time that transborder data flows and its economic and political repercussions have been 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" (Eger, 1978, pp. 1155–56). During the 1980s, international standard-setting activities took place aiming at the protection of personal data while allowing for them to be transferred abroad. Notably, the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereinafter OECD Privacy Guidelines; OECD, 1980) and the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter Convention 108; Council of Europe, 1981) have been devised with a view to creating conditions that would facilitate transborder flows of personal data (OECD, 2010a, p. 12).

As a means to this end, both international instruments set forth common data processing standards for personal information that 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, personal data sovereignty is concerned because the consequences of a loss of sovereignty are mainly borne by the individuals to whom 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, governments do not find adequate for the bulk of government information. Arguably, governmental users have different expectations of cloud services than the

majority of the individual users, for whom a change of jurisdiction and public authority does not, in most cases, 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 much governmental data, which should be an argument for ensuring a high 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 do not completely satisfy. 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 problem that transborder data flows can cause multiple jurisdictions adding-up, which causes (much-dreaded) legal complexity and, thus, uncertainty about the legal disclosure obligations on cloud service providers.

Prioritizing Interstate Mutual Legal Assistance Procedures

Interstate mutual legal assistance procedures offer an alternative mechanism to extraterritorial means of data disclosure. In order to gather forensic evidence from a cloud computing service, a foreign law enforcement agency would request assistance from a domestic law enforcement agency that has territorial jurisdiction over the cloud service operator or the data center location (Walden, 2011, p. 11). The Council of Europe's European Convention on Mutual Assistance in Criminal Matters (1959) and additional protocols provide a framework for the cooperation of law enforcement agencies across borders, and there are numerous bilateral legal assistance treaties. Using territorial jurisdiction as a default for law enforcement access to data would help reduce legal complexity and introduce transparency and procedural legitimacy to the process of seeking forensic evidence from Internet service providers such as cloud service operators.

This solution is also promoted in the 2008 Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, adopted by the global conference "Cooperation against Cybercrime" organized by the Council of Europe. Paragraph Section 36 of the guidelines holds that in a transnational constellation, law enforcement authorities should refrain from directing requests directly to nondomestic Internet service providers, but to rely on interstate procedures established in mutual legal assistance treaties (Council of Europe, 2008; see also Walden, 2011, p. 16). Hence, mutual legal assistance procedures could address some concerns over data sovereignty because they confine foreign law enforcement agencies to seek assistance from the competent authority in the country of establishment of the service provider.

However, there are a number of caveats that have rendered mutual legal assistance procedures the second best option. To start with, Walden observes that formal mutual legal assistance procedures "have historically been notoriously complex, slow and bureaucratic, which is particularly unsuitable for cloud-based investigations" (Walden, 2011, p. 11). According to legal analysts, the U.S. authorities would only revert to mutual legal assistance procedures when their

extrajurisdictional powers fail to issue a subpoena directly (Noerr SNR Denton, 2011, p. 18). On a number of occasions U.S. courts have decided that domestic discovery requests trump foreign statutes that carry provisions that prohibit compliance with foreign lawful interception regimes (Noerr SNR Denton, 2011, p. 18; Walden, 2011, p. 9).[19] Moreover, the trend to certain extra-territorial applications of lawful interception authorities is also embodied in the Council of Europe's Convention on Cybercrime (2001, Article 32).[20] The idea of strengthening mutual legal assistance procedures may therefore not be compelling to many governments, but it is still the most workable way forward.

In the literature it is controversially discussed whether for data sovereignty it would be sufficient if countries under the rule of law ensured that domestic disclosure authority over data residing in the cloud adhered to due process requirements (Rayport & Heyward, 2009, p. 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. The fundamental issue remains, however, of whether countries can entrust important government information fully to the protection of foreign jurisdictions, although it is perhaps confined to a core area in which data sovereignty prevails as a function of national sovereignty.

The European Union Digital Internal Market

For the European Union, achieving an internal market for cloud computing would be a very worthwhile policy investment in the economic prospects and competitiveness of the region. Concerns about cloud computing and the sovereignty of digital information continue to challenge the European Commission's position.[21] In her speech, the Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, emphasized the need for free flow of data across borders and between continents, while noting the trend of European Internet companies to offer European-based cloud computing services with the commercial proposition to protect users from third countries' access to their personal data (Reding, 2011b). When looking at the European Union the digital internal market with respect to cloud computing is still very much an ideal; however, European policymakers have started to explore the available instruments to achieve further integration.

In the Digital Agenda, a strategic policy paper, the European Commission recommends the development of "an EU-wide strategy on 'cloud computing' notably for government and science" (European Commission, 2010, p. 23). Neelie Kroes, the Commissioner responsible for the Digital Agenda, has made it clear that the legal framework is part of the work for the envisaged cloud strategy, focusing on an update of the European Union's data and privacy protection instruments and statutory user rights and taking into account the international dimension of cloud technology (Kroes, 2012, p. 2). The language is reminiscent of economic integration through harmonization of national laws. In early 2012, Commissioner Kroes (2012, p. 2) announced the setting up of the European Cloud

Partnership, charged with developing common requirements for cloud computing by public authorities. This partnership is not about setting up a European cloud.

Contrasting the policy development under way, the ENISA (2011, p. 9) promotes an interesting but utopian idea in its recommendation 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." The document does not elaborate further what this new cloud is about, and how it can be achieved. A supranational virtual space where all authority is exercised under a common set of rules could be a way of guaranteeing data sovereignty that is acceptable to Member States. The establishment of a similar safe harbor knows no precedent and whether such a proposal has any realistic chance of succeeding depends on many factors, but foremost if the European Union would be willing to invest its sovereignty (*regime sui generis*) in such a project.

Conclusions

If cloud computing is the next paradigm in computing, then governments cannot miss this trend—and indeed, government operations are increasingly migrating to cloud services. However, governments find themselves in the dilemma of how to benefit from cloud technology while maintaining authority over information that is increasingly abstract from physical control. This article discusses data sovereignty as a burgeoning, nonlegal, concept that is attractive to governments because it holds the promise of striking a balance between the progressing virtualization of information and their undiminishing demand for exclusive authority and control.

As an umbrella concept, data sovereignty combines principles of IT management, information assurance, and data protection, with means to address new legal risks arising from transborder transfers and the new intermediary involved, that is, the cloud service provider. The complexity of divergent, and at times conflicting, regulations of different countries is a deterrent to widespread take-up of transnational cloud services; not only for governments but for all users. These legal risks are the exposure of information in the cloud's custody to foreign jurisdictions and laws, which preempt the commercial agreement with the service provider. From a rational risk-management point of view, critical government information assets are better confined in national territory to rule out foreign jurisdictions.

This article argues that for governments the concern over national data sovereignty will persist as a function of the nation state. What ensues from the discussion of national sovereignty is that the ability to govern presupposes command and control over public sector information to the extent necessary to deliver public services and public goods, as well as to ensure the integrity of the state. In essence, national sovereignty is conditional upon adequate data sovereignty especially when ICT evolves, which would fundamentally undermine the territoriality paradigm that has traditionally ensured exclusive authority.

Given the principal nature of the concern over national data sovereignty it should be manifest in all countries' approaches to cloud computing.

A comparative analysis of Australia, Canada, the United Kingdom, and the United States shows that ultimately all these countries' cloud computing strategies have been caught by concerns about the cloud's inherent data sovereignty problem. In the United States and the United Kingdom, where government cloud services are already procured, a gradual protection of national data sovereignty can be observed. Grossly simplified, both countries allow for public cloud services at low impact levels, enforce geographical restrictions at moderate impact levels, and do not tender cloud services above moderate impact level. Given the nascent stage of development of government cloud computing these findings are preliminary, and national data sovereignty will develop a more nuanced understanding over the coming years. What emerges as a principle, however, is that data sovereignty is progressively upheld relative to the national system of security classifications for government information assets.

National data sovereignty therefore does not prevent the public sector from deploying the full range of cloud services, but not for all government information assets, and with selectively enforced geographic restrictions. This outcome is bound to contradict the cloud technology's global philosophy, although not in principle, but relative for a defined proportion of government information. As a nascent technology cloud services do nonetheless thrive on business with governments because it opens new markets where previously in-house IT services dominated in the public sector.

International and regional standard setting may alleviate some of the insecurities. However, this would not entirely resolve the problem of data sovereignty. Governments' confidence to use public cloud service more liberally could improve once the system of mutual legal assistance between countries' law enforcement agencies becomes standard procedure in addition to internationally accepted due process requirements for law enforcements' access to information in the cloud's custody. With the European cloud partnership, Member States will benefit from regional standard setting and possibly the harnessing of collective public sector buying power.

Future research on this topic could in particular investigate whether data sovereignty of nation states is eventually an extension of the concept of sovereignty. Giving consideration to the users' perspective, both government employees and members of the public would provide an additional perspective to data sovereignty. Aside from governments' needs, the concept offers a proposition how to strengthen the link between the data "owner" and 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 governance to a new level.

Notes

I am particularly grateful to Herbert Burkert, Ivan Szekely, and three anonymous referees for very useful comments on an earlier draft of this article.

1. The distinction between traditional IT outsourcing models and real cloud services can be difficult: in private clouds computing capacity is scalable, which is not the case in a dedicated private data center facility (see Armbrust et al., 2009, p. 4).
2. For a taxonomy of cloud services, see Armbrust et al. (2009), Kushida et al. (2011), and Nelson (2009).
3. In an earlier version, the NIST definition euphemistically highlighted as one advantage of the cloud paradigm that cloud software was "service oriented with a focus on statelessness" (NIST, 2009, p. 2).
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, 2009a, 2009b, 2011).
5. Note that the information assurance concept can also cover five values, that is, availability, integrity, authentication, confidentiality, and nonrepudiation (US Committee on National Security Systems [CNSS], 2010).
6. The literature discussing the bearing of cloud computing on the right to privacy and the trade-offs of international data transfers develops a similar line of argument (Jaeger et al., 2008; Nelson, 2009; Rayport & Heyward, 2009).
7. Other regulations that are much less obvious may also need to be considered. For example, in the United Kingdom when government operations migrate to the cloud this may fall under a regulation that protects employees in the case their business changes ownership, the so-called TUPE—Transfer of Undertakings (Protection of Employment) Regulations 2006.
8. The trend to open government data does not contradict data sovereignty claims but stands for the need to democratize public sector information to the widest extent possible.
9. Originally, in an official reply to the Dutch parliament of September 8, 2011 regarding the procurement of ICT services, the Dutch Minister for Security and Justice, Ivo Opstelten, declared that in order to avoid data disclosures to the U.S. authorities under the USA PATRIOT Act the contracting public authorities place a requirement on the service provider not to transfer such data. See https://zoek.officielebekendmakingen.nl/ah-tk-20102011-3516.html (in Dutch).
10. Corresponding to its statutory responsibilities for developing standards and guidelines under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.
11. 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, that is, low, medium, and high impact (FIPS, 2004).
12. http://www.gsa.gov/portal/category/102375 (accessed December 14, 2011).
13. See https://www.apps.gov.
14. According to a GSA statement the inclusion of non-U.S. data centers reflected a compromise given free trade concerns raised by other U.S. federal departments and "that it expects the non-US [option] to see very limited, if any, use" (US Government Accountability Office, 2011, p. 5).
15. The so-called G-Cloud framework accommodates services of the category Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and auxiliary services, such as data migration and integration. See http://gcloud.civilservice.gov.uk/supplier-zone/.
16. This is the case for Alberta, British Columbia, and Nova Scotia.
17. Data protection laws for the public sector can have a particularly strong impact on cloud computing. Where citizens' information protection and legal data sovereignty intersect governments are more likely to continue their own operations or to rely on regional (EEA)/domestic private cloud services which are not subject to foreign authority.
18. This does not prevent covert intelligence gathering completely. See, for example, Spiegel Online International (2010): "US Diplomats Told to Spy on Other Countries at United Nations."
19. *United States v. Bank of Nova Scotia*. 691 F.2d 1384 (11th Cir. 1982); *Columbia Pictures v. Bunnell*, 245 F.R.D. 443, 452 (C.D.Cal.2007); *Reino de Espana v. American Bureau of Shipping*, 2006 WL 3208579, *6 (S.D.N.Y. November 3, 2006).
20. For a detailed discussion on the scope and reach of the Cybercrime Convention, see Walden (2011).
21. See the official answers of the European Commission to the questions submitted by Members of the European Parliament of August 23, 2011, and November 29, 2011 (Reding, 2011a, 2011c), indicating that European law takes precedence over foreign law for entities operating in the European Union area.

References

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee et al. 2009. "Above the Clouds: A Berkeley View of Cloud Computing."

Technical Report No. UCB/EECS-2009-28 [Online]. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html. Accessed December 15, 2011.

Article 29 Data Protection Working Party. 2010. "Opinion 8/2010 on Applicable Law." WP 179. Adopted on December 16, 2010 [Online]. 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" [Online]. http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf. Accessed June 25, 2011.

Best, Jo. 2012. G-Cloud Will Lead to Shorter Contracts and IT 'Bought Like Stationary (January 26) [Online]. http://www.governmentcomputing.com/news/2012/jan/26/gcloud-contracts-liam-maxwell-procurement. Accessed January 26, 2012.

Booz Allen Hamilton. 2009. *The Economics of Cloud Computing. Addressing the Benefits of Infrastructure in the Cloud* [Online]. http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf. Accessed June 25, 2011.

Bradshaw, Simon, Christopher Millard, and Ian Walden. 2011. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology* 19 (3): 187–223.

Council of Europe. 1959. "European Convention on Mutual Assistance in Criminal Matters." CETS No. 30, entered into force June 12, 1962 [Online]. http://conventions.coe.int/Treaty/en/Treaties/html/030.htm (accessed December 13, 2011). http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf. Accessed June 25, 2011.

———. 1981. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No.: 108)." Adopted in Strasbourg, January 28, 1981 [Online]. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. Accessed June 25, 2011.

———. 2001. "Convention on Cybercrime." Adopted in Budapest, November 23, 2001 [Online]. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Accessed December 13, 2011.

———. 2008. "Guidelines for the Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime." Adopted by the Global Conference 'Cooperation Against Cybercrime' (Council of Europe, Strasbourg, France), April 1–2, 2008 [Online]. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf. Accessed December 13, 2011.

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

———. 2010. "Government of Canada (GC) Cloud Computing: Information Technology Shared Services (ITSS) Roadmap." Presentation [Online]. 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): 1065–103.

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

———. 2009b. *Cloud Computing Information Assurance Framework* [Online]. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework. Accessed June 25, 2011.

———. 2011. *Security & Resilience in Governmental Clouds* [Online]. 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) [Online]. 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* [Online]. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. Accessed June 25, 2011.

Gartner Research. 2011. *"Data Sovereignty Can Be a Hurdle for the Adoption of Cloud Computing."* July 11, 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): 269–83.

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): 6f [Online]. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171. Accessed June 25, 2011.

Klein, Kris. 2008. *Applying Canadian Privacy Law to Transborder Flows of Personal Information from Canada to the United States: A Clarification* [Online]. http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf/$file/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf. Accessed December 16, 2011.

Kroes, Nelie [Vice-President of the European Commission responsible for the Digital Agenda]. 2012. *"Towards a European Cloud Computing Strategy."* Speech at the World Economic Forum, Davos, January 27, 2012. http://europa.eu/rapid/press-release_SPEECH-11-50_en.htm. Accessed November 8, 2012.

Kundra, Vivek, and United States Chief Information Officer. 2010. *State of Public Sector Cloud Computing* (May 20) [Online]. http://www.info.apps.gov/sites/default/files/StateOfCloudComputingReport-FINALv3_508.pdf. Accessed June 25, 2011.

Kundra, Vivek, and US Federal Chief Information Officer. 2011. *Federal Cloud Computing Strategy* [Online]. 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) [Online]. http://brie.berkeley.edu/publications/wp197.pdf. Accessed June 25, 2011.

Linklaters. 2011. *Law Enforcement and Cloud Computing* [Online]. http://www.linklaters.com/Publications/law-enforcement-cloud-computing/Pages/Index.aspx. Accessed December 7, 2012.

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*. McKinsey & Co. Report (April) (On file with the author).

Microsoft Corporation. 2010. *Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing* [Online]. http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/ConfidenceWP.doc. Accessed June 25, 2011.

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

———. 2011a. *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145 (September) [Online]. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed December 14, 2011.

———. 2011b. *US Government Cloud Computing Technology Roadmap. Volume 1. High-Priority Requirements to Further USG Agency Cloud Computing Adoption* [Online]. http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf. Accessed December 14, 2012.

Nelson, Michael R. 2009. "Cloud Computing and Public Policy." Briefing Paper for the ICCP Technology Foresight Forum, OECD [Online]. http://www.oecd.org/dataoecd/39/47/43933771.pdf. Accessed June 25, 2011.

Noerr SNR Denton. 2011. *The USA PATRIOT Act. Implications for Cloud Computing* [Online]. www.snrdenton.com/PDF/USA_Patriot_Act_Cloud_Computing.pdf. Accessed December 7, 2012.

OECD. 1980. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Adopted on September 23, 1980 [Online]. 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.

———. 2010a. "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines." DSTI/ICCP/REG (2010) 6/FINAL. OECD Digital Economy Paper 176 [Online]. http://www.

oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/iccp/reg(2010)6/final&doclanguage=en. Accessed June 25, 2011.

———. 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 September 29, 2010 [Online]. http://www.oecd.org/dataoecd/27/12/45983022.pdf. Accessed June 25, 2011.

Paquette, Scott, Paul T. Jaeger, and Susan C. Wilson. 2010. "Identifying the Security Risks Associated with Governmental Use of Cloud Computing." *Government Information Quarterly* 27: 245–53.

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 [Online]. 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 [Online]. http://plato.stanford.edu/archives/sum2010/entries/sovereignty/. Accessed June 25, 2011.

PWGSC/ITSB/CTO. 2011. *IT Shared Services Security Domain & Zones Architecture*. April 20, 2011.

Rayport, Jeffrey F., and Andrew Heyward. 2009. *"Envisioning the Cloud: The Next Computing Paradigm."* A Marketspace Next Point of View [Online]. http://marketspacenext.files.wordpress.com/2011/01/envisioning-the-cloud.pdf. Accessed June 25, 2011.

Reding, Viviane. 2011a. *Answer Given by Mrs Reding on Behalf of the Commission (August 23, 2011)* [Online]. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2011-006901&language=EN. Accessed December 13, 2012.

———. 2011b. "The Future of Data Protection and Transatlantic Cooperation." Speech at the 2nd Annual European Data Protection and Privacy Conference Brussels, December 6, 2011 [Online]. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&format=HTML&aged=0&language=EN&guiLanguage=en. Accessed December 13, 2012.

———. 2011c. *Answer Given by Mrs. Reding on Behalf of the Commission (November 29, 2011)* [Online]. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2011-0085 54&language=EN. Accessed December 13, 2012.

Reed, Chris. 2010. "Information 'Ownership' in the Cloud." Queen Mary School of Law Legal Studies Research Paper No. 45/2010 [Online]. http://ssrn.com/abstract=1562461. Accessed June 25, 2011.

Reinicke, Wolfgang H. 1998. *Global Public Policy. Governing without Government*? Washington, DC: Brookings Institution Press.

Robinson, Neil, Helen R. Schindler,Jonathan Cave, and Janice Petersen. 2010. *Cloud Computing in the Public Sector: Rapid International Stocktaking. Strategies and Impact* [Online]. 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) [Online]. 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, DC, Wednesday, April 7 [Online]. 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* [Online]. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp-eng.pdf. Accessed June 25, 2011.

———. 2010. *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions* (Published 2006, amended 2010) [Online]. http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp00-eng.asp. Accessed December 16, 2011.

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

UK Cabinet Office. 2011. *Government Cloud Strategy. A Sub-Strategy of the Government ICT Strategy (March)* [Online]. http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf. Accessed December 16, 2011.

UK CIO Council. 2011. "Government ICT Offshoring (International Sourcing) Guidance." Version 1.0. July 2011 [Online]. https://update.cabinetoffice.gov.uk/sites/default/files/resources/government-ict-offshoring.pdf. Accessed December 16, 2011.

UK Department for Business Innovation and Skills. 2009. "Digital Britain." Final Report [Online]. http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf. Accessed June 25, 2011.

US Committee on National Security Systems (CNSS). 2010. "National Information Assurance (IA) Glossary." CNSS Instruction No. 4009. April 26, 2010 [Online]. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf. Accessed November 8, 2012.

US General Services Administration (GSA). 2011. "Infrastructure as a Service (IaaS). Federal Cloud Computing Initiative." GSA Blanket Purchasing Agreements Ordering Guide 2011. Version 3.0 [Online]. http://info.apps.gov/sites/default/files/IaaS%20Ordering%20Guide%2007%2001%202011%20v3.pdf. Accessed December 20, 2011.

US Government Accountability Office (GAO). 2011. *In the Matter of Technosource Information Systems, LLC; TrueTandem, LLC*. B-405296 et al., Decision of October 17, 2011 [Online]. http://www.gao.gov/decisions/bidpro/405296.pdf. Accessed December 16, 2011.

Vienna Convention on Diplomatic Relations. 1961. *United Nations Treaty Series, Vol. 500: 95* [Online]. http://untreaty.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf. Accessed June 25, 2011.

Walden, Ian. 2011. "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent." March 8, 2011. Queen Mary School of Law Legal Studies Research Paper No. 74/2011 [Online]. http://ssrn.com/abstract=1781067. Accessed December 7, 2012.

Walker, Molly B. 2011. *Kundra: Cloud Computing Data Sovereignty a Matter for 'International Law.'* (April 10) [Online]. http://www.fiercegovernmentit.com/story/kundra-cloud-computing-data-sovereignty-matter-international-law/2011-04-10#ixzz1OmRYO9fI. Accessed June 25, 2011.

Weber, Max. [1968] 1978. *Economy and Society: An Outline of Interpretive Sociology*, eds. Güther Roth and Claus Wittich. Berkeley: University of California Press.

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

———. 2010b. "Steps to Improve Cloud Computing in the Public Sector." *Issues in Technology Innovation* 1: 1–13. [Online]. http://www.brookings.edu/research/papers/2010/07/21-cloud-computing-west. Accessed June 25, 2011.

World Economic Forum. 2011. *Advancing Cloud Computing: What To Do Now*? [Online]. 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 [Online]. http://www.businessofgovernment.org/sites/default/files/CloudComputingReport.pdf. Accessed June 25, 2011.