A Change is in the Air

Emerging Challenges for the Cloud Computing Industry

Marlon Graf, Jakub Hlávka and Bonnie Triezenberg

RAND Justice, Infrastructure, and Environment, and RAND Labor & Population

WR-1144
March 2016

For more information on this publication, visit www.rand.org/pubs/working_papers/WR1144.html

Published by the RAND Corporation, Santa Monica, Calif.

Table of Contents

Acknowledgements

We wish to acknowledge the following individuals who helped us in the research process: Prof. Christopher Guo from the Pardee RAND Graduate School for helping us develop a research question that is relevant to the cloud computing industry and his facilitation of engaging classes on entrepreneurship and public policy; an academic based in Washington D.C. for insights on the future of regulation of cloud computing and data privacy in Europe and the United States; a legal expert from a Fortune 500 company based in Germany for perspective on concerns of European companies and consumers regarding usage of cloud services for storage of proprietary and consumer data; a data privacy analyst at a large technology company and cloud provider based in the Silicon Valley for perspectives on data localization, data privacy and national or international security; a manager at a large telecommunications technology company based in the Silicon Valley for insights on the challenges to cloud computing hardware manufacturers; a technology manager at a large telecommunications technology company based in the Silicon Valley for insights on technology problems and solutions associated with emerging cloud computing regulation; a senior analyst at the North Atlantic Treaty Organization based in Brussels for perspectives on government and security implications of future cloud regulations; a senior representative of an industry association concerned with the regulation of digital privacy in the United States; and a RAND researcher for contributions on the emerging legal framework to protect privacy in the United States. We also thank Rachel Swanger, Associate Dean at Pardee RAND, for a thorough linguistic review, and Liz Voss for guiding us through the publication process. Any mistakes or omissions are our own.

Introduction

With over 6 billion devices projected to be connected to the world's information superhighway in 2016 (Gartner 2015), the internet will continue to serve as a driving force for economic growth and innovation. Yet, recent developments in regulating the digital world – and cloud computing specifically –illustrate that such expansion should not be taken for granted. In fact, increasingly more restrictive measures have been imposed on digital technology providers and users world-wide, leading to a growing uncertainty about the future of digital commerce and communication. Our research indicates that while greater data localization is likely to characterize the internet of the future, new business opportunities will emerge for the providers of cloud computing technology and services.

Cloud Computing and Data Transfer

Cloud computing has been around for longer than many people think: in fact, some track its precursors to "Data Processing Service Bureaus" that were developed over 40 years ago (Hölbl 2011). In the literature, 'cloud' is defined in many different ways. We use a consolidated definition proposed by the U.S. National Institute of Standards and Technology (NIST 2011):

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Clouds can be private or public, and generally take the physical form of large server farms connected by high speed digital networks. These interconnected server farms form a "cloud" of computing infrastructure that allows users to access data, applications or simply raw computing power from nearly anywhere on the globe using relatively simple web-enabled devices. Today, some of the best-known public cloud services are offered by large multinationals and small IT companies alike. Scholarship on cloud services often describes different uses of the cloud: Infrastructure as a Service[1] (IaaS) is used by firms or consumers to obtain flexible computing resources for data storage, memory or computing power, Software as a Service[2] (SaaS) is used by firms and consumers to obtain access to software applications without having to purchase and install those application on individual devices, and Platform as a Service[3] (PaaS) is used by

[1] Such as as IBM's SoftLayer, Amazon Web Services, MS Azure, and Rackspace Open Cloud (Harmer 2015) .

[2] Such as Google Documents, SuccessFactors, Concur, and Zendesk.

[3] IBM's Bluemix, Force.com, and Google App Engine.

software developers who want to develop cloud applications without having to build the underlying software that makes cloud infrastructure accessible to the application (ibid).

In this report, we focus primarily on the IaaS use of the cloud for storage, transmission and processing of consumer and employee personal data and the ways in which that data flows across national boundaries whether in public, private or hybrid cloud deployments. While using a cloud to store, transmit and process information assures the convenient accessibility of that information independent of a user's location at a very reasonable economic cost, there are non-economic costs related to security and privacy. These addition non-economic costs may slow adoption rates of consumers or firms and may lead states to increase their regulations concerning on-line data privacy or to limit cross border flows of information. How consumers, firms and nation states think about those costs varies widely and it may be difficult to predict how regulations, norms and preferences will play out in balancing the need for privacy in information vs. the need for state and civil security in the coming years. For instance, a Pew Foundation survey of experts asked them to predict whether the world will have converged on a consensus in how best to balance privacy in the digital age and found no agreement (Rainie and Anderson 2014). Therefore, in hypothesizing how data flows across national boundaries may change in the coming years, we expanded our research to consider more than simply privacy and security regulatory reforms.

The Problem Statement

This study began in October 2015 shortly after the European Court of Justice ruled that the transfer of EU consumer data to U.S. servers under the "Safe Harbor Agreement" did not provide EU consumers with the 'equivalent protection' that they were entitled to under EU privacy laws. This led to a number of news articles and opinion pieces in various media forums, many of which saw the ruling as heralding the segregation of the internet along national or regional boundaries.[4] As part of a class in public policy analysis and entrepreneurship, the authors embarked on a study to examine the likelihood of segregation of the future internet and specifically, the impact that might have on cloud service providers. While we originally focused our attention purely on the impact of international regulatory reforms and the differences in regulation and cultural norms regarding privacy and state security among nations, we quickly came to realize that other forces were also creating a demand for what the cloud service providers refer to as "data localization". The research question was therefore generalized as: **"What are the forces that may drive demand for data localization and what are the implications of that demand for internet and cloud infrastructure providers?"**

[4] One of such pieces was published by The Economist (2015), touting a "rising fear of a balkanization of the Internet."

To answer that question, we first look at the regulatory environment and the cultural norms regarding data privacy and state or civil security in different regions of the world. We then turn our attention to the consumer demands beyond privacy that may lead to an increased demand for localized data and finally we consider the needs of corporate entities for data localization. In light of what we see as a growing demand for data localization services, we conclude with thoughts on the risks and opportunities that this change may bring to cloud service providers.

Methodology

To answer the research question posed above, the authors engaged in a series of literature reviews and semi-structured interviews with individual stakeholders. Due to the fact that this research was conducted as an unfunded class assignment over the course of six weeks, we were unable to interview a large number of stakeholders. However, we strove for diversity of viewpoints and read widely on the subject. While we acknowledge that the following discussion is EU and U.S.-centric, it was often our research into trends in non-EU and U.S. countries that drove our conclusions.

High-Level Findings

We find that there are significant market forces which may drive cloud services and the internet infrastructure towards increased data localization. We anticipate that the combination of technical need, consumer privacy concerns, state security concerns and corporate confidentiality needs will lead to an increased demand for contractual and technical mechanisms to ensure that data is kept within specific geographic and/or national boundaries. We further anticipate that there will be a growth in market demand for local or regional data centers, for software or hardware that facilitates geographic localization, and for services that audit the geographic routing of data, the authentication of those who access data and more convenient and secure encryption of data both at rest and in transit. Innovations in these areas may provide firms with large payouts in the coming years.

Europe and the United States

As the largest economy in the world, the European Union is rightly concerned with its competitiveness in the digital world, and has proactively pursued policies that promote legal certainty while adhering to its founding principles of human dignity, liberty, democracy, equality, the rule of law and respect for human rights. Its cornerstone documents include references to privacy, such as Articles 7[5] and 8[6] of the EU Charter of Fundamental Rights on Data Protection and the Respect For Private and Family Life.

In September 2012, the European Commission adopted a strategy for ”Unleashing the Potential of Cloud Computing in Europe” (European Commission 2012) which aimed at maximizing the “potential offered by the cloud”, and started working with a number of stakeholders and advising bodies, including the European Union Agency for Network and Information Security (ENISA). One of the main fora to discuss cloud-related concerns and regulations is the European Cloud Partnership (ECP) and its Cloud-for-Europe (C4E) initiative (European Commission 2015).

Safe Harbor

As a supranational entity, the European Union adopts regulations and directives that are binding to its member states. The European Union's Directive on Data Protection (95/46/EC) regarding personal data transfers to third countries, which came into effect in October 1998, allows the transfer of “personally identifiable data to third countries only if they provide an "adequate" level of privacy protection” (Aaron 2000). As a result, an agreement was proposed by the United States Department of Commerce to allow U.S.-based companies to exchange private data with their European counterparts without interruptions. In July 2000, the European Union approved the ‘Safe Harbor Agreement’ (formally expressed in Commission Decision 2000/520/EC) with the United States, and it came into force four months later. Based on this agreement, companies covered by its stipulations were to be considered as providing ‘adequate’ data privacy protection – and data transfer from the European Union to these companies would

[5] Full Text of Article 7: *Everyone has the right to respect for his or her private and family life, home and communications.*

[6] Full text of Article 8: *1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*

continue unhindered (Aaron 2000). Yet, on October 6, 2015, this agreement was struck down by the Court of Justice of the European Union (CJEU) on the grounds of insufficient ability to exercise national oversight over data transfer in the current system (CJEU 2015). CJEU argued that:

> (…) national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements (ibid).

'Safe Harbor 2.0' was negotiated by European and U.S. authorities with a self-imposed deadline in January 2016.[7] European Union's Commissioner for Justice, Consumers and Gender Equality, Věra Jourová from the Czech Republic, noted that in principle, an agreement has been reached, but that parties had been "discussing how to ensure that these commitments are binding enough to fully meet the requirements of the [CJEU ruling]" (Moody 2015). At a November 2015 event at the Brookings Institution in Washington D.C., she expressed support for the Judicial Redress Act that is currently being discussed in the United States (Brookings Institution 2015). She also highlighted that the European Union would require safeguards on private data from all countries going forward, emphasizing the need for detection and supervision mechanisms based on "transparency, enforcement and redress" (ibid).

Despite promising signs emanating from the recent negotiations, representatives of 28 EU data protection authorities warned that:

> (…) if by the end of January 2016, no appropriate solution is found with the U.S. authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions (Article 29 Working Party 2015).

In the meantime, it has been reported that German authorities were investigating large U.S. technology companies, including Facebook and Google, about their data transfer practices and that potentially, court orders to halt these transfers may be imposed (Moody 2015). Hamburg's Commissioner for Data Privacy and Freedom of Information, Johannes Caspar, noted that the best solution for technology companies dealing with the personal data of European citizens is to "consider storing [them] only on servers within the European Union" (ibid). Several technology companies, including Twitter, took precautionary measures before the ruling was reached, introducing new privacy policies and likely moving data to different servers ahead of the ruling (Anthony 2015).

---

[7] Please note this working paper was finished before a new agreeement was reached on February 2, 2016, and reflects the situation before the new agreement. Although the issue of storing and transferring EU citizen information within private companies on U.S. servers has been temporarily resolved, we do not believe that fact negates the findings of our research.

An expert we interviewed observed that a new agreement would be extremely difficult to renegotiate as the European Union has effectively ruled that it cannot trust its citizens' data will not be mishandled by U.S. intelligence services: any future alternative agreements may be subject to the same challenge unless the American security apparatus makes radical changes to how it operates. A further observation was made that localized regulation is unlikely to lead to widespread industry relocations or disruptions – while more data centers may need to be located in Europe, they are unlikely to create significant new employment as their maintenance is largely automatized and core innovation will take place in existing technology hubs.[8]

The Safe Harbor ruling, however, is a significant setback for politicians who aim to facilitate international trade and investment. One expert argued that the ruling, a decision of the CJEU, reflects a markedly different perception of privacy adequacy in Europe. That perception has likely escalated the issue more substantively than a political body like the European Parliament would have.[9]

United States

The U.S. Constitution does not explicitly recognize a fundamental right to data privacy for individuals. Instead, the U.S. has developed a patchwork of laws and regulations that protect privacy in different circumstances. Laws protecting against data collection by government entities are centered on the Fourth Amendment to the U.S. Constitution, which guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". As interpreted by the Supreme Court, this right only applies when government action violates a reasonable expectation of privacy (REOP). Whether that right extends to data stored in the cloud has yet to be fully tested and it appears that arguments will be based on whether or not U.S. consumers lose their REOP when they share their data with third parties.[10] Laws protecting against data collection by private entities vary depending on a number of factors, including the type of information collected, the entity collecting the information, the individual the information is collected from, and the jurisdiction in which the information is collected. These privacy laws are generally considered weaker than their European equivalents and, except for some particularly sensitive types of information, often rely on self-regulation from the entity collecting the data. For the U.S. consumer who has chosen, perhaps unwittingly, to allow on-line companies to amass and mine her personal data, it often feels that the adage "possession is nine-tenths of the law" is all that applies as those firms assert their "ownership" of that data.

---

[8] Phone interview with the research team on December 2, 2015.

[9] Ibid.

[10] A good description of the history and implications of the "third party doctrine" and its implications for state access to personal information in the U.S. have been summarized by Villasenor (2013).

While the U.S. government was originally deeply involved in the development and governance of the internet,[11] the existing infrastructure was privatized in the mid-1990s and governance today is largely under the auspices of the Internet Society (ISOC), an international body with membership open to any individual and, for a fee, any organization. Since privatization, the U.S. government has taken a hands-off approach in regulating the development of new innovation based on internet-enabled communication and has no comparable body to the EU's ECP forum for guiding the development of cloud technologies. In 2014, the National Institute of Standards and Technology (NIST) published a technology roadmap for the U.S. Government's use of cloud technologies which focused primarily on security and interoperability and was based on working groups convened with industry representatives in 2010 and 2011 (Badger et al. 2014). While one intent of the NIST roadmap is to impact and foster communication regarding commercial, government and international development and uses of the cloud, the roadmap itself applies only to U.S. Government agencies.

Snowden Revelations

In the wake of the terrorist attacks on September 11, 2001, the Patriot Act was adopted in the United States, giving the government the ability to collect information about U.S. citizens and foreigners without consent and with limited oversight over search warrants. Although the Patriot Act is the most well-known of the regulations allowing the U.S. government to access information collected by commercial entities that supply mobile telephone, internet, search and cloud services, there are other regulations that also give them access via subpoena, warrant or sometimes simply by asking. The depth of the U.S. Government's access to personal data came to light when Edward Snowden revealed information detailing the extent of the U.S. National Security Agency's (NSA) activities. These revelations made concrete the fears of many internet users, both inside and outside the U.S., that their information was readily available to U.S. government agencies.[12] For EU privacy advocates, they constituted a "proof" that EU personal data stored by U.S. internet and mobile service providers did not offer the equivalent protection as data stored within the EU.

Judicial Redress Act of 2015

The Judicial Redress Act of 2015 is an attempt by the U.S. Congress to address some part of the cross-border data transfer issues. This bill would allow foreign citizens in European countries to sue the United States for unlawful disclosure of personal information—under the terms of the

[11] The internet as we know it was governed by the U.S. National Science Foundation from its infancy in the early 1980s until its privatization in the mid-1990s.

[12] For a contemporaneous view of the worldwide impact that Snowden had on perceptions of government spying, see a survey published by the Pew Research Center (2014).

Privacy Act—obtained in connection with international law enforcement efforts. Under the current law, only U.S. citizens and legal residents can bring claims against the federal government for unauthorized disclosure of their personal information. While this bill passed the House in October of 2015, it remains in the Senate Committee on the Judiciary and has not been brought to the floor for a vote.[13]

Even if passed, it should be noted that the Judicial Redress Act does nothing to change the regulatory environment in the United States. Non-U.S. citizens would need to sue under U.S. law with its reliance on third party doctrine and the REOP principle. These protections are hardly equivalent to existing EU law.

[13] Progress of this bill can be tracked at: https://www.govtrack.us/congress/bills/114/hr1428

Other Regions

While the majority of cloud computing technologies and regulations have origins in the United States and Europe, other regions of the world have played important roles in the developments of digital privacy protections. We focus on Russia, China and the largest Latin American economies given the broad spectrum of data protection they manifest and the role they play in the public discourse in both Europe and the United States.

Russia

Russian laws passed in 2005 and 2006 establishing the data rights of individuals to their personal information mirror those of the EU on paper. Under those laws, "opt-in" is the default standard for consent—especially for marketing purposes, Russian citizens have the right to know what data is collected about them by commercial entities and have the right to know how it is processed.[14] Data of Russian citizens may be taken out of the country, but only to countries which have agreed to the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*

In September 2015, a new amendment to Russia's Personal Data Protection Act went into effect, requiring that personal data of Russian citizens must be stored on Russian servers. Although cross-border transfer remains legal, the amendment also gives Russia more power to block sites that it believes are "illegally" processing its citizens' data. How Russia intends to implement these laws is a subject of great concern and uncertainty to many multinational firms, not just cloud providers.

It should be noted that "state secrecy data" is exempt from the Personal Data Protection laws —although Russian citizens are protected from unwanted surveillance by commercial firms, there are no protections from electronic surveillance by Russian state entities (Practical Law 2015).

China

China does not have personal data protections laws similar to those found in the EU and in Russia. Nor do they have a general law restricting cross-border transfers of personal data. However, some laws do exist for some specific types of data. For instance, data collected by commercial banks cannot be transferred across borders. A similar prohibition applies to any data involving state secrets.[15] Chinese citizens have no protections from unwanted surveillance by either commercial firms or by Chinese state entities. Non-Chinese citizens should not expect

[14] For an English language overview of Russian data protection laws, see Practical Law (2015).

[15] For an English language overview of China's data protection laws see Practical Law (Practical Law 2015a).

their data to remain private if transferred to servers in China or if their data transits through Chinese internet or wireless services.

Latin America

Several sources confirm that while many Latin American countries have privacy provisions in their regulations or even constitutions, enforcement is largely absent or only selectively applied (Cruz 2012). *Figure 1* summarizes the current regulatory environment in the largest five Latin American economies with respect to international data transfers. In the next section, we describe some of the specifics of these differences.

Figure 1: Cross-Border Data Transfer in Largest Latin American Economies

Brazil	Brazilian law does not expressly restrict cross-border data transfer. A **new privacy law** currently under development requires an adequate level of protection: "International transfer of personal data is only allowed for countries that provide a level of protection for personal data that **is equivalent to the level established in this Law**" (Ministry of Justice of Brazil 2015) It further requires that "A country's level of data protection shall be assessed by the competent body" (ibid). For non-compliant countries, a specific consent to transfer data would be required (ibid).
Mexico	Requires "**notice and consent of the data subjects**" but does not require an adequate level of protection in the recipient country (IT Law Group 2014).
Argentina	Personal Data Protection Law N° 25.326 from 2000 states that "The transfer of any type of personal information to countries or international or supranational entities which do not provide **adequate levels of protection**, is prohibited," but does not specify how adequacy is established (Proteccion de datos personales 2000).
Colombia	According to Law 1581, Article 26, cross-border transfer of data can only be performed to a country with a **comparable level of data protection** (El Congreso de Colombia 2012). This can be superseded by an express and unequivocal consent to the transfer or when the transfer is necessary for the fulfillment of a legal or contractual obligation (Sanlate et al. 2013).
Venezuela	Venezuela Law **does not have a specific regulatory framework** for data protection. There are provisions dealing with privacy rights in various laws, including: the Telecommunications' Privacy Protection Law; the Defense of Access to Goods and Services Law; the Data Messages and Electronic Signatures Law; the Special Law on Computer Crimes; and the Labor Working Environment and Working Conditions Law (D'Ambrosio 2013).

Brazil

Brazilian law requires no contractual obligations regarding cloud-based services but it explicitly states that any collection, storage and use of personal data by connection providers and on-line application providers must comply with the "rights to privacy, to protection of personal data, to secrecy of private communications and of logs" (ICLG 2015). Article 5 of the Brazilian Constitution refers to the inviolability of "privacy, private life, honour and image of persons" (Brazilian Chamber of Deputies 1988).

In February 2015, a draft of Brazil's first comprehensive privacy law was issued, defining key terms like "consent", "personal data", "sensitive personal data" and others, as well as rules on intra-company and international data transfers. This draft allows the processing of data "transferred to Brazil from other jurisdictions, where the relevant consent requirements (if any)

of the country of origin are satisfied" (Yalamova 2015). Enforcement issues have not been fully resolved but the draft included a requirement that companies processing personal data develop sufficient information security measures and appoint a dedicated privacy officer (ibid).

Mexico

Similarly, Latin America's second largest economy adopted the 'Federal Law on the Protection of Personal Data held by Private Parties' in July 2010 with additional regulations issued in December 2011 (Perspecsys n.d.). Inspired by a Spanish precedent, the Mexican law now covers 'collection, use, disclosure, storage, access, management, transfer and disposal of personal data' but lets companies define their data protection policies (ibid). One of the solutions devised by organizations in the country includes replacing sensitive data by tokens that are stored in the cloud: thus, sensitive data remains under the control of the company (ibid). Sometimes, encryption is used. For cross border data transfers, the law requires "notice and consent of the data subjects" – this is in contrast to European Union's Data Protection Directive, for instance, which also requires an adequate level of protection in the recipient country (IT Law Group 2014).

Argentina

Analogously to Mexico, Argentina adopted the Personal Data Protection Law N° 25.326 in 2000, drawing on its Spanish equivalent. Since then, however, only a very small portion of databases with personal information stored in them has been registered with the National Directorate for Personal Data Protection (DNPDP) as the law requires (Milanés 2015). Similarly as in European law, the Argentinian Personal Data Protection Law prohibits the "transfer of personal data to countries that do not have an adequate level of protection in place", however a definitive list of these countries has not yet been compiled (ibid). Furthermore, very few companies in the country comply with ISO/IEC 27018, the newest business standard in cloud privacy.[16]

[16] "ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment." (ISO 2014)

Global Regulatory Environment

As the above examination of the regulatory environment for data transfer and privacy illustrates, countries are addressing the issues at hand in divergent ways: some countries such as the United States and China lean towards low levels of restrictions of who can access and use personal data contained within the networks and servers that make up the cloud infrastructure, while other countries, mainly led by European Union member states, are pushing for an increase in data protection measures for the sake of personal privacy. While European and Latin American countries' support for enhanced data protection measures resulted from debates around privacy and security in the cloud, other countries such as China and Russia have been equally strong in their opposition of international data transfers, albeit for national security reasons.

While regulations and enforcement differ widely around the world, some platforms, such as Practical Law's website, provide up-to-date overviews of data transfer regulations. A query requesting a comparison of laws regulating cross-border data transfers[17] shows that most countries have restrictions of some type. In response to these regulations, localized data storage has emerged as a mitigating strategy, with data centers geographically distributed across the world to set up regional cloud computing hubs.

Data Centers World-Wide

The functioning of today's on-line services requires widespread infrastructure, particularly in the form of data centers and their connections to the consumers. In our interviews with industry representatives, we found that geographic proximity is particularly important in voice and streaming services that are sensitive to latency (delays between client requests and the responses of cloud service providers) and jitter (deviations or displacements of signal pulses caused by electromagnetic interference and other factors). To mitigate the risk of natural disasters or other disruptions in data center operations, it is common to require that data be stored in at least two different locations. To understand the impact of data localization regulations, we examined the current geographic distributions of data centers world-wide.

Today, the majority of data centers are located in the developed world, chiefly in Europe and North America, as existing statistics show (we use the Data Center Map, a comprehensive database of 3,768 data centers world-wide, but are aware that some data centers may not be included). *Figure 2* shows the distribution of colocation data centers in the world, weighted by population. *Figure 3* shows the top 20 countries with the most colocation data centers on their territory in absolute terms.

---

[17] An example of such a query is http://bit.do/practicallawcomparison.

Figure 2: Colocation Data Centers World-Wide, Population-weighted (Data Center Map 2015, World Bank 2015)

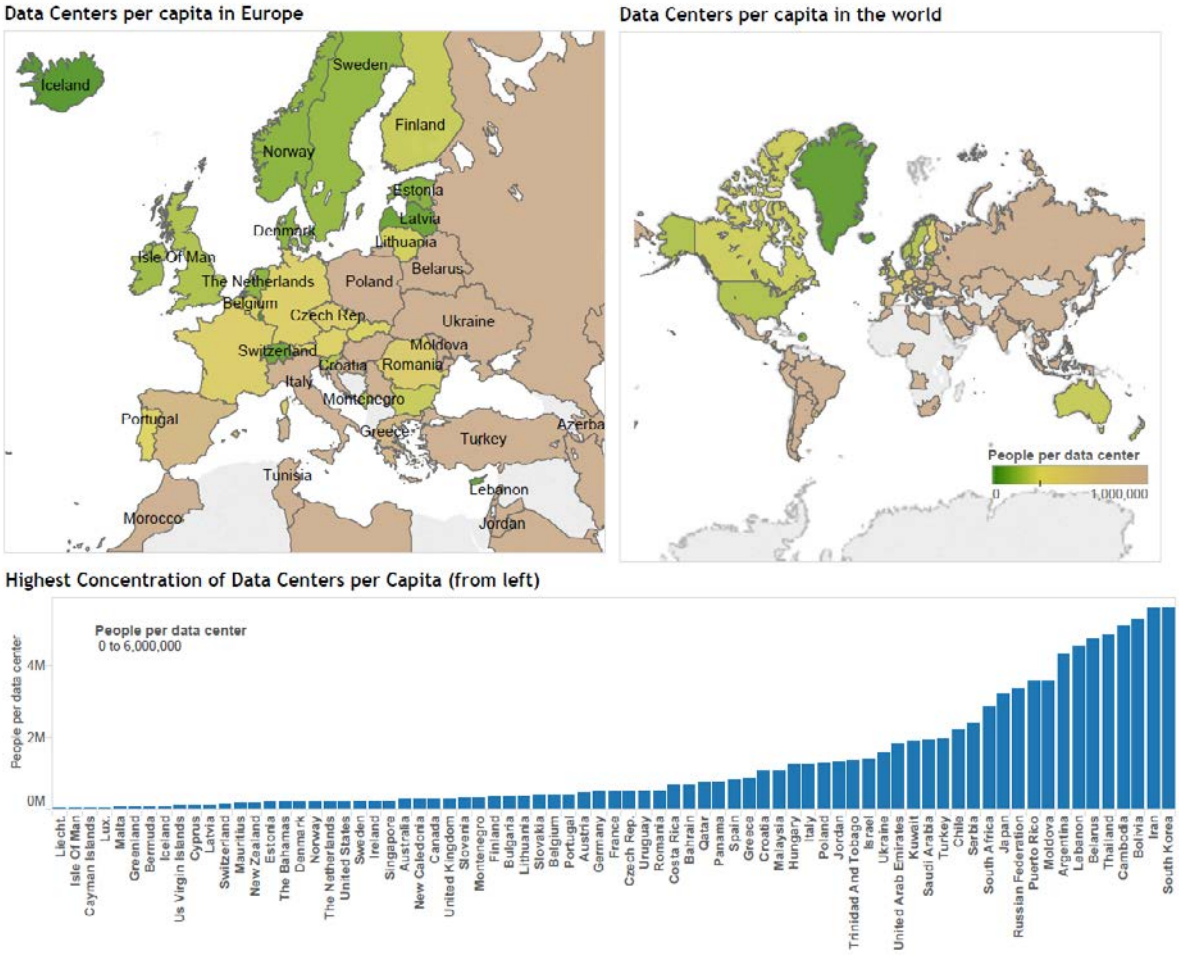
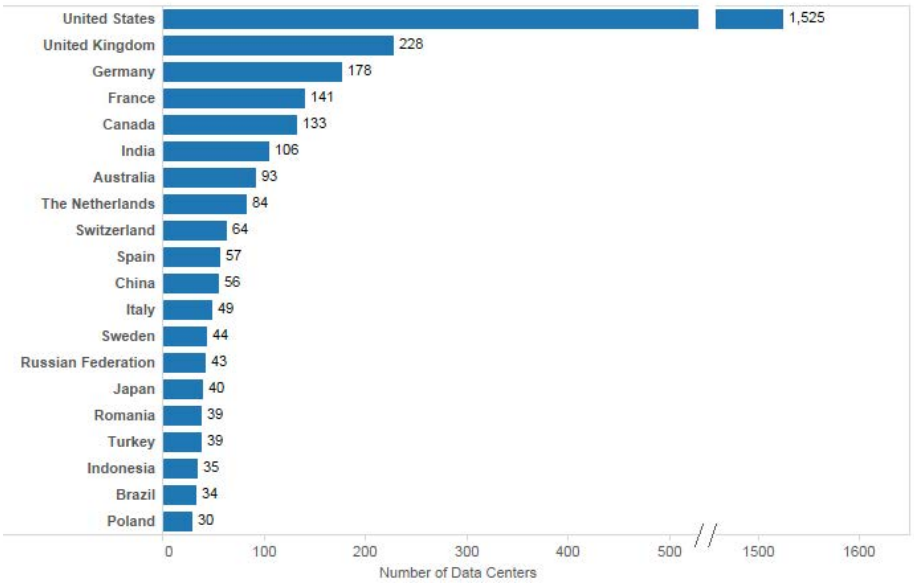
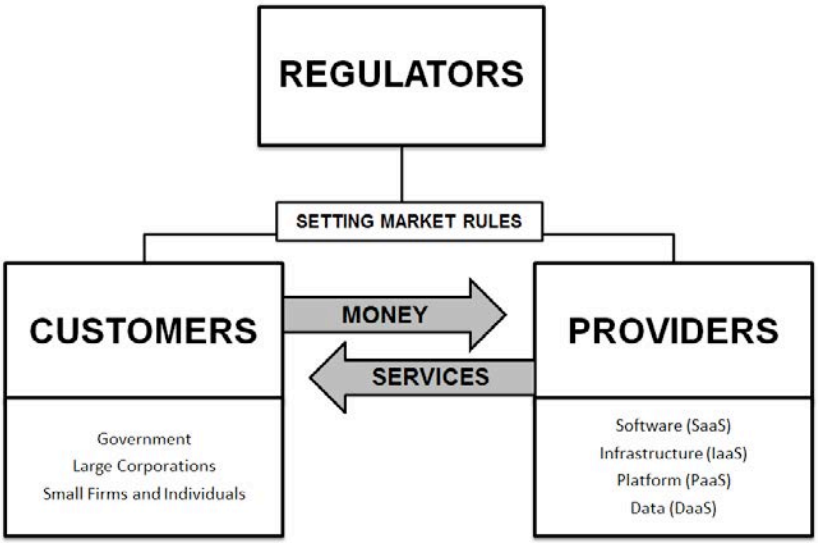


Figure 3: Countries with Most Data Centers in the World



In seeking to understand the cloud computing industry, we began by closely examining the various actors involved in the market. As articulated by Leimeister (2010), the value network of cloud computing consists of providers, consultants and customers, while regulators establish the rules of interaction between these actors. A schematic of the market structure for cloud computing is presented in *Figure 4* below:

Figure 4: Cloud Computing Industry Market Structure



Cloud providers

Providers in the cloud computing industry typically offer a variety of services and products such as lending infrastructure or computing capacity (IaaS), offering software as a service (SaaS) or storing and analyzing data (DaaS) (Armbrust 2009, Dillon 2010). Effectively, cloud service providers' business models can be classified as either horizontal or vertical integration.

Vertical Integrators

Vertical integrators are focused on specific industries, offering highly specialized solutions. The main advantage of this approach is the high degree of market penetration that can be achieved. For instance, Bloomberg and the financial industry offer a suite of products that is tailored specifically to firms in one industry and they have become the standard operating platform for that industry. Given that there are commonly a few key customers and at most a few rival providers, it is relatively easy to navigate the market and to adjust to new needs and trends.

On the other hand, there are some limits to vertical integration: most often, growth opportunities are tightly tied to the evolution of a small, yet a high-value market.

Horizontal Integrators

Conversely, horizontal integrators such as Google or Amazon offer basic, broad solutions for customers across a variety of industries. This approach can be best characterized as utility computing, with low margins and low market shares, but also a very large potential for cost-sharing and economies of scale. Horizontal integrators benefit from a vast customer base.

Depending on the size and resource stock of a specific provider, it may be beneficial to pursue either business model, although the utility-like model poses relatively higher barriers to entry given the large upfront investment necessary (The Economist 2015a).

Cloud customers

When looking at customers of cloud computing services, one can broadly differentiate between three key groups of clients:

- large corporate clients,
- small firms or individuals, and
- government agencies.

Depending on the type of customer, various aspects of cloud computing are perceived as clear advantages, as opportunities or even challenges and threats. We illustrate the benefits, opportunities and challenges associated with the cloud in *Figure 5*.

Figure 5: Pivotal Issues in Cloud Computing

WHAT'S GREAT ABOUT THE CLOUD?	WHAT'S UP FOR DEBATE?	WHAT'S BAD ABOUT THE CLOUD?
Turning infrastructure investment into operating cost: • Lower barriers to market entry • Flexible and demand-specific capacity / usage • Scalability • Ability to reach customers online	**Data security:** • For small firms, data much safer on the cloud • For large firms, not necessarily the case **Enhanced data mining:** • Good for advertising and law enforcement • Seen by many as invasion of privacy	**General lack of regulation:** • Who is liable if there is a data breach (provider or data owner)? • Who should be able to access data? • How will the Safe Harbor ruling affect future cloud computing investment?

The primary advantage of cloud computing is that it brings down the costs of conducting business by turning large, up-front, fixed cost investments in IT infrastructure into variable operating costs (Etro 2009). In addition, relying on cloud computing resources leads to increased flexibility and the ability to rapidly scale up capacity and usage. As an example, one could easily imagine a startup beginning with just a few computing resources and then rapidly expanding to keep pace with their growing customer base by purchasing extra capacity on the cloud when faced with a spike in demand. Furthermore, renting flexible cloud computing allows firms to adjust their capacity according to seasonal demands – one good example is a tax business that needs of a lot of capacity during tax season but much less during the rest of the year.

All of these advantages apply universally to cloud computing customers, including large corporations and government agencies. The most significant benefits, however, are reaped by small firms and individuals. The opportunity to access high level computing resources cheaply and quickly substantially lowers their barriers to market entry. All that is really required to launch a business is access to a computer or tablet; large infrastructural investments are no longer necessary. Aside from this cost-cutting advantage, it has now become much easier to reach niche customers on a global scale—cloud-based firms have the ability to offer solutions for a much broader variety of computing problems and markets and can find the small subset of customers looking specifically for those types of tailored solutions. As an example, many small firms are now able to provide highly specialized user interfaces for cloud computing services such as Amazon Web Services or other applications that are of high use to very small groups of users.

The main reason many customers, both corporate and individual, rely on cloud-based solutions is the promise of large cost savings. On this particular issue, experts appear to be in consensus. However, when considering other aspects of cloud computing, the attitudes of large corporation and small firms or individuals differ dramatically.

Data Security

The first of these issues is data security (Bisong 2011). For a small firm, data are probably safer in the cloud than on their own servers. Google, Amazon and other providers have many more resources and it is their core business to deal with data security on an everyday basis. For large corporations on the other hand, storing data in the cloud means giving up control and not knowing where data are stored exactly or what specific measures providers are employing to ensure data security. For large corporations, this represents an essential tradeoff between cost reduction and control, while small firms do not necessarily have to worry about control due to the fact that defaulting to cloud provider practices presents their best available alternative in terms of data security and computing efficiency.

Data Mining and Analytics

The second issue is related to enhanced data mining and analytics. The rise of data analytics has created a number of new opportunities in cloud computing: advertisers can customize what they offer, law enforcement agencies can operate more effectively and even politicians can use social media analytics (as seen in the voter targeting used in Barack Obama's Presidential campaigns and in most electoral campaigns since then). Despite these opportunities, data mining has been met with great skepticism by society. In Europe particularly, many people view personal data as their property and do not want others to use it for anything or even have access to it. Although U.S. citizens do not have this same right of data ownership, they are sensitive to having their private data used for commercial gain, especially without their knowledge.

While cloud customers are heavily divided on issues such as data security and data mining or analytics, there appears to be overwhelming consensus on the negative effects of lack of regulation and resulting uncertainties (Kaufman 2009).

Data Transfer

Data transfer needs are increasingly global but, as we described in the regulatory section above, many regions such as Russia, China, Latin America and Europe are beginning to issue restrictive rules for cloud computing providers. Particularly for globally operating entities, this is creating a whole new set of challenges. Where firms used to be able to rely on the provisions of the Safe Harbor Agreement, the European Court of Justice by striking down the agreement effectively created a legal void that has made it more difficult to operate internationally and across national borders.

Intra-Company Data Transfer

Our interviews suggest that, given recent regulatory developments, large multi-national corporations that hold customer and employee data from multiple countries are mitigating their risk of possible lawsuits by 1) isolating their Russian activities and 2) using one of two solutions for handling of EU citizen data; either they apply for self-binding rules with extremely high standards and commitments to data protection and obtain approval from an EU-based data protection agency, or they rely on standard contract clauses where all processes that involve data transfer include special data protection procedures and guidelines. Even before the Safe Harbor agreements were struck down, we learned that most corporate customers who use private cloud services structure their contracts to restrict storage of their data to specific geographic locations. If a replacement for the Safe Harbor Agreement is developed in the near future,[18] some of the stimuli driving data localization may be reduced, but we are not convinced they will disappear

[18] Please note this working paper was finished before a new agreement was reached on February 2, 2016, and reflects the situation before the new agreement.

entirely. Having done the hard legal work to assure greater control of data, multi-national companies may be loath to give it up.

B2C Data Transfer

In addition to intra-corporate transfer, there are issues surrounding the relationship between cloud customers and cloud providers. Rules for data access and liability, in particular, are handled somewhat ambiguously. The consequences of data breach or loss are often outlined through the cloud provider's Service Agreement Terms, typically requiring providers to handle the data with reasonable care, but negating responsibility in case anything goes awry – thus leaving blame and damages with the customer (Hackett 2014). Additionally, it is frequently unclear how access to data is handled, especially given the increased demand for access from law enforcement agencies and the recent spike in cyber terrorism. In the future, corporate clients might start to push for more private space on public clouds such as Amazon Web Services, asking providers to "lose the key" and to refrain from even looking at the actual data (Hofmann 2009).

More Storms for Cloud Computing are on the Horizon

Ultimately, when looking at the demand side of the cloud computing market, it seems clear that while there are undeniable cost savings and enhanced business opportunities associated with its expansion, a great deal of uncertainty, particularly in terms of regulation of intracompany and B2C transfers, remains. The differential treatment of cloud computing issues in various countries presents substantial challenges to all stakeholders and might benefit from some level of agreement on the basic framework for data transfers and data privacy in the cloud. This may not be as unrealistic as it seems given the relative similarity of privacy preferences among the citizens of the most advanced economies.

Cultural Aspects of Privacy Regulation

The increased debate surrounding data privacy regulations, and the divergent positions taken by the European Union and the United States in particular, raise the question whether the differences are too stark to be reconciled. If European citizens simply care more about their privacy for one reason or another, it is hard to imagine any kind of convergence leading to a regulatory solution on the international stage. Nonetheless, as evidenced by the growing cloud computing industry described above, market forces will continue to push towards the elimination of legal uncertainties. To evaluate the tradeoffs between globalized data transfers on one end and citizens' concerns for data privacy and protection on the other end, this chapter assesses regional variations in preferences related to data privacy, transfer and cloud computing.

Data Privacy, State Security and the 'Willingness to Trade Privacy'

Digital commerce is growing rapidly around the world, even on the crisis-stricken Old Continent: the trade association *Ecommerce Europe* estimates that the internet economy was worth 2.2% of the continent's GDP in 2013 and will double by 2016 and triple by 2020 (Crisp 2014). Given this growth, it is perhaps not surprising that an increasing number of European consumers expresses concern about the security of their personal data stored on-line.

The EU is not a monolith, however, and Europeans differ slightly in their perspectives on data privacy. This is illustrated by the EMC's Privacy Index which collected data in 15 countries world-wide and showed that while only 12% of Germans were willing to trade privacy for convenience, almost a third of Italians were ready to do so (the global average was 27%) (EMC Corporation 2014).

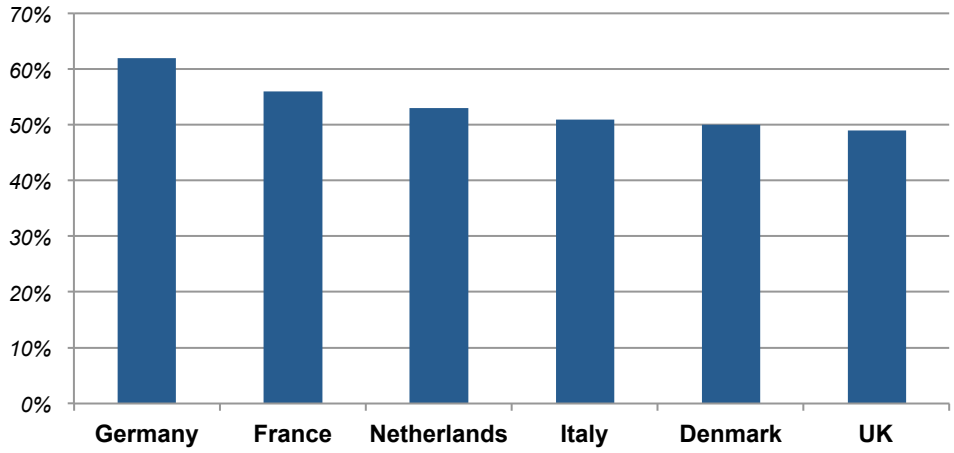
Figure 6 shows selected results for all countries in the study based on a sample of 15,000 respondents (1,000 in each country, margin of error 3.1%). There is relative similarity of consumer preferences in most European countries, the United States, Canada, Australia and New Zealand. The statistics are led by traditionally risk-averse Germans, with the French, Australians and New Zealanders, Canadians and Brits in close proximity. In contrast, we observe most of the developing world, with consumers in India, the Middle East, Russia and Mexico, much more willing to trade their privacy for the convenience that the internet and cloud can bring. While we can expect fluctuations in perceptions across the board, particularly due to domestic political developments, the data indicate that the greatest demand for privacy solutions will originate from the most advanced economies: the EU, Canada, Australia/New Zealand, and the United States.

Figure 6: EMC Privacy Index

	% of Respondents "willing to trade privacy for convenience"	% of Respondents who Think Selling and Buying Private Data Should Require Opt-In	% of Respondents Who Think Privacy Will be More Difficult to Maintain in the Next 5 years	% of Respondents Who Have Experienced a Data Breach
Germany	12%	92%	88%	42%
France	15%	91%	84%	45%
Australia/NZ	15%	93%	89%	50%
Canada	17%	92%	85%	56%
United Kingdom	18%	91%	84%	52%
USA	21%	88%	85%	58%
Netherlands	23%	94%	89%	38%
Brazil	26%	89%	73%	76%
China/HK	29%	88%	79%	68%
Italy	29%	88%	86%	43%
Middle East	32%	71%	70%	67%
Japan	33%	91%	90%	18%
Russia	38%	92%	81%	61%
Mexico	43%	87%	73%	75%
India	48%	78%	59%	64%
GLOBAL Average	27%	87%	81%	>50%

Similar conclusions were reached by Symantec (2015): 88% of European consumers consider data security 'very important' in choosing the company to buy products from (more than the quality of the product itself or the customer service, which are 'very important' for 86% and 82% of Europeans, respectively) (ibid, 37). Moreover, Symantec's survey indicated that 50% of European respondents were willing to pay for data protection at the level of credit card insurance payments, and 46% the same or more than their monthly cellular service (ibid, 28). These preferences seem to reflect the fact that 59% of respondents have had an experience with a data breach, and 57% of them believed that their data were not safe. *Figure 7* summarizes which European citizens have the greatest concerns about the safety of personal information.

Figure 7: Percentage of European Respondents Concerned about Data Privacy and Information Safety (Symantec 2015)



The attitudes of U.S. consumers are not so different from those in the EU countries. Dr. Alan Westin conducted a number of privacy preference studies between 1978 and 2003 and divided the U.S. population into those who are *rarely* willing to trade, those who are *almost always* willing to trade and those who are *sometimes* willing to trade convenience for privacy (the Privacy Pragmatists). Over the years the studies were conducted, the number of pragmatists grew as people became more aware that a trade is being made (Kumaraguru 2005). A more recent study by the PEW Research Center after the Snowden revelations showed that about 75% of respondents thought it was very important to control who had their information and only approximately 25% of them trusted their mobile and internet service providers to protect their data (Pew Research Center 2015b).

In 2014, a software market analyst firm surveyed U.S. adults to find out how they felt about the European Union's "right to be forgotten" which had recently been upheld by the Court of Justice of the European Union. The ruling gives European citizens the right to request that their personal data be delisted from search engines. 61% of U.S. respondents want some form of the EU's right to be forgotten, 39% want the U.S. to adopt a European-style right to be forgotten, without restrictions, and 47% were concerned that "irrelevant" search results can harm a person's reputation. In their analysis, the firm concluded that responses were driven more from a desire for privacy than a desire to be forgotten (Software Advise 2014).

Cultural Consequences of Providing Greater Data Protections

While many cloud computing providers are based within the U.S., regulation of data protections, and hence of cloud computing, is chiefly driven by regulatory authorities outside the United States. Europe seems to be leading the way, with much of Latin America following its lead. Yet the difference in attitude towards privacy between United States, EU and Latin American citizens are strikingly small. In other words, the differences in regulations appear to be driven much more by the legal frameworks and fundamental rights statements of these countries than by the current attitude of the citizenry. A cloud computing company that met the EU legal obligations for protection of individual data should be able to capitalize on those sentiments to capture market share in both the U.S. and world's emerging markets, barring the most restrictive markets like Russia.

We conclude that while regulations of data privacy and security differ significantly world-wide, the European Union is in a particularly strong position to shape the regulatory environment in cloud computing given the growing demand for more reliable privacy protections and the relative similarity in privacy preferences within the developed world. With its stricter requirements for data privacy and security, the European model presents the industry with significant short-term challenges limiting the ability to freely transfer sensitive information. However, this trend has the potential to create lucrative business opportunities in the long-term.

Conclusions

A Push Towards Data Localization

As this report has shown, we see national regulations as a significant force leading to greater data localization. However, we also find that not all forces leading towards data localization are regulatory. As shown in *Figure 8*, consumer preferences for data privacy, national security concerns in countries like Russia and China, liability concerns of business entities and even the growth of data streaming and voice applications all drive the need for data localization services.

Figure 8. Non-Regulatory Drivers of the Need for Data Localization Services

With respect to global regulatory trends, a clear consensus has emerged in our interviews: national regulations governing data transfer and privacy will not significantly converge in the foreseeable future. With comprehensive privacy rights enshrined in its founding documents, the European Union continues to enforce data protection through its courts. On the other hand, the U.S. offers no similarly broad basis for digital privacy in its laws and the U.S. Congress has yet to pass the Judicial Redress Act of 2015, though its protections are not on par with its European counterparts. Latin American countries, while formally guaranteeing many of the same rights as European laws, have been largely unable to effectively enforce them. Finally, both Russia and China appear to be moving towards the isolation of their digital infrastructures.

A Regulatory Turf War

P.W. Singer and Allen Friedman point to a growing competition to regulate the Internet between the ISOC (current regulators), the International Telecommunications Union (ITU) and

individual countries (Singer and Friedman 2014). The ISOC, with its open and non-representative membership and consensus-driven decision making processes, is viewed by many countries as being too closely aligned with the large internet providers and with U.S. interests. Yet, most countries appear to be aware of the advantages that global connectivity has provided to their economies and to their overall interests. They see the continued need for such a body in regulating protocols, domain services and guaranteeing interoperability. For many countries, the ITU, with its closed national membership and traditional emphasis on respecting national differences and on using votes rather than consensus to reach decisions (it is part of the United Nations system), is a more appealing venue for regulation. Certainly, any move that appears to bolster the role of the ITU in internet regulation should be viewed as a sign that the forces leading to greater data localization are strong enough to significantly shape the future of the internet and of cloud computing.

Risks and Opportunities for Cloud Providers

In our study, we find there are significant market forces driving cloud services and the internet infrastructure towards increased data localization. We anticipate the combination of technical need, consumer privacy concerns, state security concerns and corporate confidentiality needs will lead to an increased demand for contractual and technical mechanisms to ensure data are kept within specific geographic and/or national boundaries. We further anticipate there will be growth in market demand for local or regional data centers, for software or hardware that facilitates geographic localization, and for services that audit the geographic routing of data, the authentication of those who access data and more convenient and secure encryption of data both at rest and in transit. Innovations in these areas may provide firms with large payouts in the coming years.

Undoubtedly, the fragmentation of the internet will increase the costs for cloud computing providers. However, given the already extensive data center buildout across the globe, these costs do not appear unmanageable. While new hardware investment may be necessary in light of emerging regulation around the world, we did not observe a clear consensus among the experts we interviewed about the magnitude of additional costs imposed by stricter data and privacy regulations. There is an opportunity for cloud providers in that many consumers, and especially corporations, may be willing to pay for assured localization and higher security standards of their data.

From a societal point of view, the transaction costs of transferring data across national boundaries will undoubtedly increase, but these costs may be offset by decreases in intellectual property piracy and increased protection of personal data. Additional research should be conducted to inform how liability for data breaches and other adverse consequences of imperfect data protection can be addressed by regulators and what technical steps the industry can take to improve the way it handles sensitive personal data. This will eventually lead to new business

opportunities for those providers who adapt to the new reality – particularly as solutions with higher privacy protections become the standard in the market and consumers demand better services from cloud computing providers. The industry is likely to undergo a major adjustment in the next decade but there is no reason to become pessimistic about the human ability to innovate and adjust to new circumstances.

Bibliography

Aaron, David L. "Cover letter from Ambassador David L Aaron to US organizations requesting comments on the newly-posted draft documents." *Letter* . March 17, 2000.

Anthony, Sebastian. *ArsTechnica.* October 6, 2015. http://arstechnica.co.uk/tech-policy/2015/10/europes-highest-court-strikes-down-safe-harbour-data-sharing-between-eu-and-us/.

Armbrust, Michael, O. Fox, Rean Griffith, Anthony D. Joseph, Y. Katz, Andy Konwinski, Gunho Lee et al. "Above the clouds: a Berkeley view of cloud computing." 2009.

Article 29 Working Party. *Hunton Privacy Blog.* October 16, 2015. https://www.huntonprivacyblog.com/files/2015/10/20151016_wp29_statement_on_schrems_judgement-2.pdf.

Badger et al., Lee. "US Government Cloud Computing Technology Roadmap Volume I." *NIST Special Publication 500-293.* National Institute of Standards and Technology. Gaithersburg, MD, October 2014.

Bisong, Anthony, and M. Rahman. *An overview of the security concerns in enterprise cloud computing.* arXiv preprint arXiv:1101.5613, 2011.

Brazilian Chamber of Deputies. "Constitution of the Federative Republic of Brazil." *Tribunal Superior Eleitoral.* 1988. http://english.tse.jus.br/arquivos/federal-constitution (accessed 2015).

Brookings Institution. *Brookings.edu.* November 16, 2015. http://www.brookings.edu/events/2015/11/16-future-us-eu-data-transfer-arrangements.

CJEU. *Europa.eu.* October 5, 2015. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

Crisp, James. "Asia-Pacific outstrips Europe as world's largest e-commerce market." *euractiv.com.* June 2014. http://www.euractiv.com/sections/innovation-enterprise/asia-pacific-outstrips-europe-worlds-largest-e-commerce-market-302859.

Cruz, Xath. *Data Protection and Privacy Issues in Latin America.* November 21, 2012. http://cloudtimes.org/2012/11/21/data-protection-privacy-issues-latin-america/ (accessed 2015).

D'Ambrosio, Nick. *Tips for Coping with Global Data Privacy Regimes.* KPMG. 2013. http://www.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/Utilities-Energy-Compliance-Ethics/2013/Tuesday/402handout.pdf (accessed 2015).

Data Center Map. *Colocation Data Centers.* December 2015. http://www.datacentermap.com/datacenters.html (accessed December 2, 2015).

Dillon, Tharam, Chen Wu, and Elizabeth Chang. " Cloud computing: issues and challenges. ." *Advanced Information Networking and Applications , 24th IEEE International Conference* . Ieee, 2010.

El Congreso de Colombia. *Ley Esta Tutaria 1581: Por la cual se dictan disposiciones generales para la protección de datos personales.* Bogotá, 2012.

EMC Corporation. *EMC Privacy Index.* 2014. http://www.emc.com/campaign/privacy-index/global.htm (accessed 2015).

Etro, Federico. "The economic impact of cloud computing on business creation, employment and output in Europe." *Review of Business and Economics* , 2009: 54.2, 179-208.

European Commission. *Digital Agenda for Europe.* Februrary 27, 2015. https://ec.europa.eu/digital-agenda/en/european-cloud-initiative.

European Commission. "Unleashing The Potential Of Cloud Computing In Europe." *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions* . Brussels , September 27, 2012.

Gartner. *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015.* November 2015. http://www.gartner.com/newsroom/id/3165317 (accessed January 2016).

Hackett, Robert. *Despite risks, businesses store sensitive data in the cloud unprotected.* May 2014. http://fortune.com/2014/05/02/despite-risks-businesses-store-sensitive-data-in-the-cloud-unprotected/ (accessed January 2016).

Harmer, Bil. *Clearing the Air Around Cloud Computing.* November 30, 2015. http://data-informed.com/22115-2/?sf16307243=1 (accessed December 1, 2015).

Hofmann, Paul, and Dan Woods. "Cloud computing: the limits of public clouds for business applications." *Internet Computing, IEEE* , 2009: 14.6: 90-93.

Hölbl, Marko. *Cloud Computing Security and Privacy Issues.* Council of European Professional Informatics Societies, Brussels, Belgium: CEPIS, 2011.

ICLG. *iclg.co.uk.* 2015. http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/brazil.

ISO. "ISO/IEC 27018:2014." *Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* Geneva, 2014.

IT Law Group. "Mexico's New Federal Law on the Protection of Personal Data." *IT Law Group.* 2014. http://www.itlawgroup.com/resources/articles/98-mexicos-new-federal-law-on-the-protection-of-personal-data (accessed 2014).

Kaufman, L. M. "Data security in the world of cloud computing." *Security & Privacy, IEEE*, 2009: 7(4), 61-64.

Kumaraguru, P. and L.F. Cranor. "Privacy Indexes: A Survey of Westin's Studies." 2005.

Leimeister, Stefanie, et al. "The Business Perspective of Cloud Computing: Actors, Roles and Value Networks." ECIS, 2010.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. "Cloud computing—The business perspective." *Decision Support Systems*, 2011: 51(1), 176-189.

Milanés, Valeria Natalia. *Intellectual Property and Technology Journal.* 2015. http://www.iptjournal.com/protecting-personal-data-in-argentina-a-work-in-progress/.

Ministry of Justice of Brazil. "Draft Law on the processing of personal data to protect." Brasília, 2015.

Moody, Glyn. *ArsTechnica UK.* October 27, 2015. http://arstechnica.co.uk/tech-policy/2015/10/germany-to-begin-investigating-legality-of-eu-us-data-transfers-immediately/.

NIST. "NIST Special Publication 800-145." *The NIST Definition of Cloud Computing* . September 2011. 2.

Perspecsys . "Data Privacy Laws & Cloud Adoption in Mexico." *Perspecsys* . n.d. http://perspecsys.com/data-privacy-laws-cloud-adoption-in-mexico/ (accessed 2015).

Pew Research Center. *American Attitudes About Privacy, Security and Surveillance.* May 20, 2015b. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (accessed Dec 2015).

—. *http://www.pewglobal.org/2014/07/14/nsa-opinion/table/country-citizens/.* 2014. http://www.pewglobal.org/2014/07/14/nsa-opinion/table/country-citizens/ (accessed January 2016).

PEW Research Center. *The Future of Privacy.* Decemeber 18, 2014. http://www.pewinternet.org/2014/12/18/future-of-privacy (accessed Dec 2015).

Practical Law. *Data protection in China: overview.* New York, NY, 2015a.

Practical Law. *Data protection in Russian Federation: overview.* New York, NY, June 2015.

Proteccion de datos personales. *Personal Data Protection Act 25.326.* 2000. http://www.protecciondedatos.com.ar/law25326.htm (accessed 2015).

Rainie, Lee, and Janna Anderson. *Privacy in 2025: Experts' Predictions.* December 2014. http://www.pewinternet.org/2014/12/18/privacy-in-2025-experts-predictions (accessed January 2016).

—. *The Future of Privacy.* Pew Research Center. December 2014. http://www.pewinternet.org/2014/12/18/future-of-privacy (accessed January 2016).

Robinson et al., Neil. *The Cloud: Understanding the Security, Privacy and Trust Challenges.* RAND Europe with time.lex and University of Warwick, 2010.

Sanlate et al., Geida. *Colombia Adopts Regulations to Implement its Data Protection Laws.* 2013. https://www.littler.com/colombia-adopts-regulations-implement-its-data-protection-laws (accessed 2015).

Simmons, Richard, and Katie Wike. *Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech.* Washington D.C., November 2015.

Singer, P.W. and Allan Friedman. *CyberSecurity and CyberWar; What Everyone Needs to Know.* New York: Oxford University Press, 2014.

Software Advise. *US Attitudes Toward the "Right to be Forgotten" - Industry View.* September 2014. http://www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/ (accessed Dec 2015).

Symantec. *State of Privacy Report 2015.* Mountain View, CA: Symantec, 2015.

The Economist. "New EU privacy rules could widen the policy gap with America." *The Economist.* October 2015. http://www.economist.com/news/international/21671081-court-ruling-october-6th-could-alter-way-data-flow-around-internet-new-european-privacy (accessed December 2015).

—. *The cheap, convenient cloud.* April 2015a. http://www.economist.com/news/business/21648685-cloud-computing-prices-keep-falling-whole-it-business-will-change-cheap-convenient (accessed January 2016).

Vaquero et al., L.M. "A Break in the Clouds: Toward a Cloud Definition." *ACM SIGCOMM Computer Communication Review* 39, no. 1 (2009): 50-55.

Villasenor, John. "What You Need to Know about the Third-Party Doctrine." *The Atlantic* . Washington, DC, December 2013.

World Bank. *Data.* December 2015. http://data.worldbank.org/indicator/SP.POP.TOTL (accessed December 2, 2015).

Yalamova, Maria-Martina. *InsidePrivacy.* April 14, 2015. http://www.insideprivacy.com/international/brazil-extends-the-consultation-period-on-its-draft-data-protection-law-until-april-30/.