Collaborating for Competitiveness

**No.:102/TRAI/2016-17/ACTO**
**Dated: 08th August, 2016**

**Shri A. Robert J. Ravi**
**Advisor (QoS)**
Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan,
Jawahar Lal Nehru Marg,
New Delhi-110002

**Subject: ACTO's response to TRAI Consultation Paper dated 10th June 2016 on Cloud Computing**

Dear Sir,

Association of Competitive Telecom Operators (ACTO) is pleased to submit its response to TRAI Consultation Paper on Cloud Computing.

We hope that our comments (enclosed as Annexure – I supported with annexure-II & III) will merit consideration of the Hon'ble Authority.

Thanking you,
Respectfully submitted

Yours sincerely,
for Association of Competitive Telecom Operators

**Tapan K. Patra**
**Director**

Encl: As above

Collaborating for Competitiveness

**Annexure-I**
**ACTO's response on TRAI CP on Cloud computing**

We welcome the opportunity to submit our comments on the Consultation Paper on Cloud computing issued by Telecom regulatory Authority of India (TRAI). Cloud computing is increasingly being adopted by businesses, including SME's and large enterprises, to benefit from the adoption of technology which is scalable, flexible, cost efficient and enhances the end user experience.

Cloud computing was recognized as an important emerging technologies and services format under the National Telecom Policy of 2012 (NTP 2012). The Government's prestigious Digital India Program can be realized with the widespread adoption of cloud computing. It should be noted that emerging IoT/M2M services also too depend on cloud computing, particularly to store and manage data collected from sensors and machines in a secured manner.

Cloud computing can play an important role for achieving economic development goals in emerging markets like India by furthering public welfare, reducing access costs, and enabling more efficient service delivery. The adoption of these technologies / services will help provide the much needed push to the growth of data and broadband services principally by reducing computing costs for end users.

**Impetus to Cloud Computing under National Telecom Policy-2012 (NTP – 2012)**

NTP-2012 has recognized the growing importance of cloud-based applications and services in accelerating the design and roll out of the new and innovative services on large scale. Importantly, the NTP 2012 has recognized the need to reduce regulatory barriers that could impede the adoption of cloud computing in India.

The policy has further noted that Cloud computing will significantly speed up ability to design and roll out services, enable social networking and participative governance and m-Commerce at scale which were not possible through traditional technology solutions.

***10. CLOUD SERVICES***
*10.1. To recognise that cloud computing will significantly speed up design and roll out of services, enable social networking and participative governance and e-Commerce on a scale which was not possible with traditional technology solutions.*

*10.2. To take new policy initiatives to ensure rapid expansion of new services and technologies at globally competitive prices by addressing the concerns of cloud users and other stakeholders including specific steps that need to be taken for lowering the cost of service delivery.*

*10.3. To identify areas where existing regulations may impose unnecessary burden and take consequential remedial steps in line with international best practices for propelling nation to emerge as a global leader in the development and provision of cloud services to benefit enterprises, consumers and Central and State Governments.*

*11.3. To adopt best practices to address the issues (like encryption, privacy, network security, law enforcement assistance, inter-operability, preservation of cross-border data flows etc.) related to cloud services, M2M and other emerging technologies to promote a global market for India.*

The advent of technologies like cloud computing present a historic opportunity to catapult India's vaunted service delivery capabilities to a new level domestically as well globally.

The NTP-2012 further recommends that the government implement measures to facilitate a liberalized regulatory environment that will foster affordable, reliable and secure telecommunication and broadband services across the entire country.

**Issues for consultation-:**

The following issues have been identified for the public consultation by TRAI and we would like to submit our responses in-seriatum:

**Question 1. What are the paradigms of cost benefit analysis especially in terms of:**
**a. accelerating the design and roll out of services**
**b. Promotion of social networking, participative governance and e-commerce.**
**c. Expansion of new services.**
**d. Any other items or technologies. Please support your views with relevant data.**

**ACTO Response:**
Recent analyst report provides interesting insights on paradigms of cost benefit analysis in terms of expansion of new services. Cloud is now an integral part of enterprise IT and Enterprises are looking for cloud solutions that will help make their businesses more efficient, agile, responsive, and competitive.

Cloud is now firmly established as a reliable enterprise workhorse, and what's most interesting is how it is driving transformation. Organizations are using the cloud to create new customer experiences, re-engineer their business processes and find new opportunities to grow. Organizations are not just using more cloud based technologies; They are using it for applications which are more demanding and more critical to everyday operations and performance. This often includes multiple mission-critical applications. Advances in technology are changing the cost-benefit equation and making it easier for companies to build more powerful environments in the cloud, enabling them to move more workloads and transform more processes. Request to refer a report on "**State of the market: Enterprise Cloud 2016" by Verizon** is attached as **Annexure –II**.

**Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organization?**

**ACTO Response**:
While business of all size benefit from the efficiencies of cloud services, the most impactful dimension of cloud services in cost reduction is actually the benefit to small businesses, where cloud services can spare these businesses from incurring the upfront cost of building an IT infrastructure and enable them to use standard applications off the cloud.

**Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?**

**ACTO Response**:
Several factors influence business enterprise decisions, depending on which on type of solution is preferred, capital and expense budgets and the degree of in-house technical expertise. As with any enterprise grade service, security, resilience, scale, flexibility and cost are important factors.

There are various other parameters that the business enterprises focus on while selecting type of the cloud service deployment model. As per a recent study, Hybrid cloud

deployment model is now the mainstream. The decision to move to hybrid cloud is influenced by several considerations.

Advances in technology are changing the cost-benefit equation and making it easier for companies to build more powerful environments in the cloud, enabling them to move more workloads and transform more processes.

It's been suggested that hybrid cloud which is the use of a mix of models, including on-premises and public and private cloud will become mainstream within five years. We think that it already is, especially for large organizations. There are already services that enable companies to create a sophisticated environment made up of multiple clouds from multiple providers, but make it look like a seamless part of the enterprise infrastructure.

**Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?**

**ACTO Response**:
Encryption **is** one of the critical components of digital security which is the ability to use robust encryption. Therefore the government should adopt a flexible approach to encryption that help ensures the security of data transfer, processing and storage. Telecom licensees should similarly be allowed the flexibility to use higher encryption to build security into the core of their network and services.

**Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?**

**ACTO's Response**:
The regulatory provisions should offer complete flexibility to move the data as the ability for information to flow across borders will be increasingly important to economic growth as all businesses are dependent on the flow of digital, cloud-based information.

As recognized worldwide, the ICT services have important multiplier effects across other economic sectors and thus play an important role in stimulating broader economic activity. As digital services and global access to the Internet expand, there are enormous opportunities for economic growth. Thus the regulatory provisions should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services. In addition, governments should not give priority or preferential treatment to national suppliers of ICT services in the use of local infrastructure, national spectrum, or orbital resources. The same should be based on user preference and choice depending the individual parameters and technical competence.

Given the rapid pace of innovation in digital technology and services, governments are urged to maintain a light touch regulatory approach to avoid stifling growth in the digital economy. It is important that governments find a balance that enables adequate protection for data without burdening industry with unworkable data privacy and protection obligations.

**Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?**

**ACTO Response**:
Cloud services as a new sourcing and delivery model is being adopted on a global scale and is becoming a business transformation technology. The regulatory framework and standards

should promote open standards based cloud infrastructure that will help increase software and data interoperability. Governments should take a light touch approach that enables industry to invest and develop new and innovative cloud technologies. Technical standards should be the domain of industry and locally prescribed standards should be avoided to enable global interoperability.

**Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.**

**ACTO Response:**
Cloud Service providers typically provide their services to other businesses rather than end users directly. As such, QoS is a matter of contractual negotiation between the two parties. Any disputes arising over QoS would be settled according to the arbitration arrangements stipulated under the contract. Given the globally competitive marketplace for cloud services, government regulation of cloud computing is not necessary.

TRAI should avoid any mandated service quality levels for cloud services. These services are different services from traditional Telephone Services, relying on fundamentally different technology and featuring myriad different service attributes and configurations, with different capabilities and limitations and raising different policy considerations.

**Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?**

**ACTO Response:**
As noted in the answer to Question 7, Cloud Computing services are generally provided to business and are the result of negotiated contracts. Any questions regarding billing would be addressed under the contract itself. Disputes would be resolved in accordance to the terms of the contract. Given the globally competitive nature of cloud computing, its regulation in this matter is not deemed necessary.

**Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.**

**ACTO Response:**
As addressed above, most cloud computing services are offered to enterprises, but in the instances where cloud services are offered on a retail basis to individual customers, existing consumer protection laws as applicable to ICT sector are sufficient to deal with any complaints or grievances over related to a cloud service.

Additionally in majority of cases these are issues between service providers and enterprise and multinational companies, which are contractual issues that do not require intervention from regulators.

**Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.**

**ACTO Response:**
**Need for flexible approach to encryption that allows for use of strong and robust encryption.** A flexible approach to encryption that enables the use of strong encryption technologies needed to ensure cloud services are secure. The government should aim at

introducing a encryption policy which enables maximum flexibility and empowers the growth of cloud services. We urge the Government to adopt a flexible encryption policy so that cloud service providers can offer services using robust encryption in India.

**Question 11. What are the termination or exit provisions that need tobe defined for ensuring security of data or information over cloud?**

**ACTO Response:**
The existing provisions under the information Technology Act 2000 related to data privacy are sufficient to deal with the security of data or information over cloud.

**Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?**

**ACTO Response:**
Given the ever changing cyber security landscape, contractual arrangements between cloud service providers and enterprises are best suited to provide the flexibility to adopt new security practices in any migration of data between or to a cloud-based service.

**Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider(CSP); and (b) End users?**

**ACTO Response:**
As stated previously, most cloud service providers provide services to an enterprise, not necessarily to an end user directly. As such, contractual arrangements are sufficient to address issues of security. In the instances where a cloud service provider may provide services on a retail basis to individual consumers, the terms of service shall delineate the roles and responsibilities with respect to security. Given the globally competitive nature of cloud based services, in both instances there should be significant competitive market pressures on cloud service providers to ensure robust security.

**Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?**

**ACTO Response:**
Seamless flows of information across borders are essential to growth throughout the global economy, since services, manufacturing, and even agriculture increasingly rely on digital communication and other data transfers. The cloud frameworks should avoid and eliminate barriers to these data flows. Further the regulatory framework for cloud and other emerging technologies should be such that it enables the service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in the cloud.

The success of the cloud computing industry depends on the global interoperability of services and the free movement of data across borders, as well as robust protections for the privacy and security of customers' data. Consumers rightly expect that the information they entrust to cloud service providers will be highly secure and that CSPs will be respectful of their privacy. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Establishing this trusted environment for consumers is crucial to the success of the market, separate and apart from the policy frameworks for privacy and security issues.

Governments can build trust in the cloud computing industry by ensuring that cloud service providers follow industry best practices and guidelines regarding the use and protection of personal data. The consultation paper cites the frameworks developed by the Asia Pacific Economic Cooperation (APEC), the Organisation for Economic Co-operation and Development (OECD), and the International Conference of Data Protection and Privacy Commissioners (the Madrid Resolution of 2009), which serve as widely accepted international standards for multinational companies that collect, use, and transfer data, as well as for states when facilitating the transfer of data across borders. Rather than erecting barriers to cross-border data flows, the TRAI should ensure that cloud service providers in India adhere to principles such as these and provide strong accountability mechanisms for customers and others who wish to challenge data management practices.
It will be a paradox like situation, support for open internet while put restriction on cross border data flow or insisting for data localization.

The growth of the Internet has also entailed the growing ability of people, businesses, and governments to collect, share, and use data across borders. The development of new technologies, products, and services in recent decades would never have been possible without the ability to freely move data across borders. Combining globalization with new technology and with new business models has dramatically accelerated the pace of change and innovation.

Cross-border data flows have also been a driving force behind the emergence of so-called global value chains in which businesses' operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production. The flow of data is as important as the movement of goods. Data needs to move to create value. Data sitting alone on a server is like a static /storage library where it's information flow is restricted and against value addition to foster innovation. It may be safe and secure, but largely stagnant and underutilized.

Some may have a belief that Data localization increases security but on the contrary, Data security depends on a plethora of controls, not on the physical location of a server. Businesses often back up data outside the country in which it is collected to help ensure it remains secure in the event of a natural disaster, power outage or other such emergency that could take a data center offline. Businesses and consumers benefit when those who maintain data are able to use the best available security measures, regardless of the physical location of the data they seek to protect. Geographic neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions. Limiting the private sector's ability to transfer, store, and process data across borders will somehow protect user privacy and improve security but these well-meaning efforts are ultimately counterproductive. The movement of data is no less important to the global economy than the movement of money. Cross-border data flows, just like cross-border financial flows, allow companies to integrate their personnel, manage their global supply chains and customer networks, and maintain the competitiveness they need to grow and thrive. The free movement of data is fully compatible with legitimate security concerns.

There are people who advocate for Data localization because it will promote domestic industry. On the contrary, data localization requirements reduce competitiveness by walling off domestic businesses from the billions of potential customers outside of the home country's borders. This isolation reduces investment and access to capital – the ability to assess a potential borrower's creditworthiness or to spot potentially fraudulent activity often depends on the ability to move data across borders.

TRAI consultation paper also indicates the fact that the growth of cloud services in EU is not in line with other counties by having strict regulation in EU in cross border data flow.

We request to refer to an important paper on "***The Cost of Data Localization: Friendly Fire on Economic Recovery"*** released by ECIPE(European Centre for International Political Economy) to provide a holistic view ill effects on any regulation mandating data localization is attached as **Annexure-III**.

**Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?**

**ACTO Response:**
The institutional framework to access data in other countries should be based on mutuality and reciprocity. The scope of bilateral and multi-lateral agreements may be enhanced for sharing information based on principles of transparency and accountability. Finding a balance is important if the full benefits of international trade in goods, services and e-commerce are to be realized by reducing unnecessary costs of doing business. Transparent and efficient mechanisms based on the rule of law are critical to building trust between countries in this area.

We note that this principle was recently upheld in the United States where a court ruled that law enforcement authorities cannot compel a U.S.-based company to turn over the data of a non-U.S. citizen for data held outside of the United States.
Please see Verizon's public policy blog on the decision at:
http://www.verizon.com/about/news/verizons-transparency-report-microsoft-case-and-icpa

Governments should ensure that clear and transparent legal frameworks address the means by which law enforcement authorities obtain access to data stored by companies. Governments can also foster a successful cloud computing industry by committing to use existing Mutual Legal Assistance Treaties (MLATs) and processes when they seek access to data that is stored beyond their borders.

**Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations there under?Please comment with justification.**

**ACTO's Response:**
In our view for continued adoption of Cloud computing services these should be left outside the purview of license or registration. International experience has demonstrated that light touch regulatory framework has fostered the growth of new technology and services.

Specific to the Indian scenario the adoption of cloud computing is still at a nascent stage and catching up with the new set of opportunities and challenges as jurisdiction over data in the cloud has been a cause of concern for regulators globally. However the concerns can be addressed through mutuality and reciprocity rather than prescriptive licensing requirements.

Some of the noteworthy forward-looking government initiatives such as Digital India, MeghRaj, and Smart Cities are a step in the right direction to increase cloud awareness and adoption and any efforts to bring the Cloud services under the ambit of a license or registration could be counterproductive and would not be conducive to the growth of the sector.

**Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?**

**ACTO Response**:
In our view, to encourage cloud services, Government of India should look at, Light touch regulations that create an enabling regulatory environment for proliferation of Cloud services as per the objectives set out in the National Telecom Policy 2012.

The institutional framework to access data in other countries should be based on mutuality and reciprocity. The scope of bilateral and multilateral agreements may be enhanced for sharing information based on principles of transparency and accountability.

Government authorities should ensure that clear and transparent legal frameworks address the means by which law enforcement authorities obtain access to data stored by companies. They should also commit to using existing MLAT processes in order to obtain data that is stored beyond their borders.

**Question 18. What are the steps that can be taken by the government for:(a) promoting cloud computing in e-governance projects.**
**(b) promoting establishment of data centres in India.**
**(c) encouraging business and private organizations utilize cloud services**
**(d) to boost Digital India and Smart Cities incentive using cloud.**

**ACTO Response:**
Some of the noteworthy government visionary initiatives Digital India, MeghRaj, and Smart Cities Mission are a step in the right direction to increase cloud awareness and adoption.

In our view, the Government of India should follow international best practices for cloud adoption and applications by Government in this regard. There are already Public Private Partnership (PPP) models that demonstrate the value of collaboration with the industry.

We recommend that the Government of India establishes a public private partnership process that helps establish Indian government security performance expectations in the context of globally recognized information security standards such as ISO 27000, and enables cloud vendors to receive certification by reputable 3rd party auditors (regardless of their nationality.

**Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?**

**ACTO's Response:**
Generally, the answer would depend on the scope of users (government or public) and the sensitivity of the functions. There could be different costs associated with these different approaches.

**Question 20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?**

**ACTO's Response:**
The availability of a robust underlying network infrastructure which is scalable to cater to the cloud requirement is very critical. In addition, the government of India needs to continue to focus on creating an investment climate that addresses key infrastructure improvements in power, land ownership, taxes etc.

**Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?**

**ACTO Response**:
Government should encourage development of cloud infrastructure by providing tax incentives as well as take a light touch approach to regulation in the ICT sector to enable adoption of cloud across the Indian economy.

It is important that TRAI also develops a light touch regulatory framework for cloud services that can help ensure the on-going, robust network deployment necessary to support this technology into the future. TRAI must minimize regulatory burdens, and provide policy certainty that will create the climate to maximize essential infrastructure investment. The key attributes of that framework should include:

- Support for the collaborative, self-regulatory initiatives among industry stakeholders In areas where regulatory action may be justified, use of a light touch, flexible, well co-ordinated regime that protects innovation and facilitates rapid cloud market developments;
- Clear and transparent rules governing law enforcement access to data

Creating conducive environment for having data centre in the country is a much superior approach than to restrict cross border data flow or to force for data localization. Data centre business/investment will flow as an automatic choice as business needs for. For example Singapore in Asia is a preferred choice for setting up data centre in APAC region. In India, we need to address the issues like:

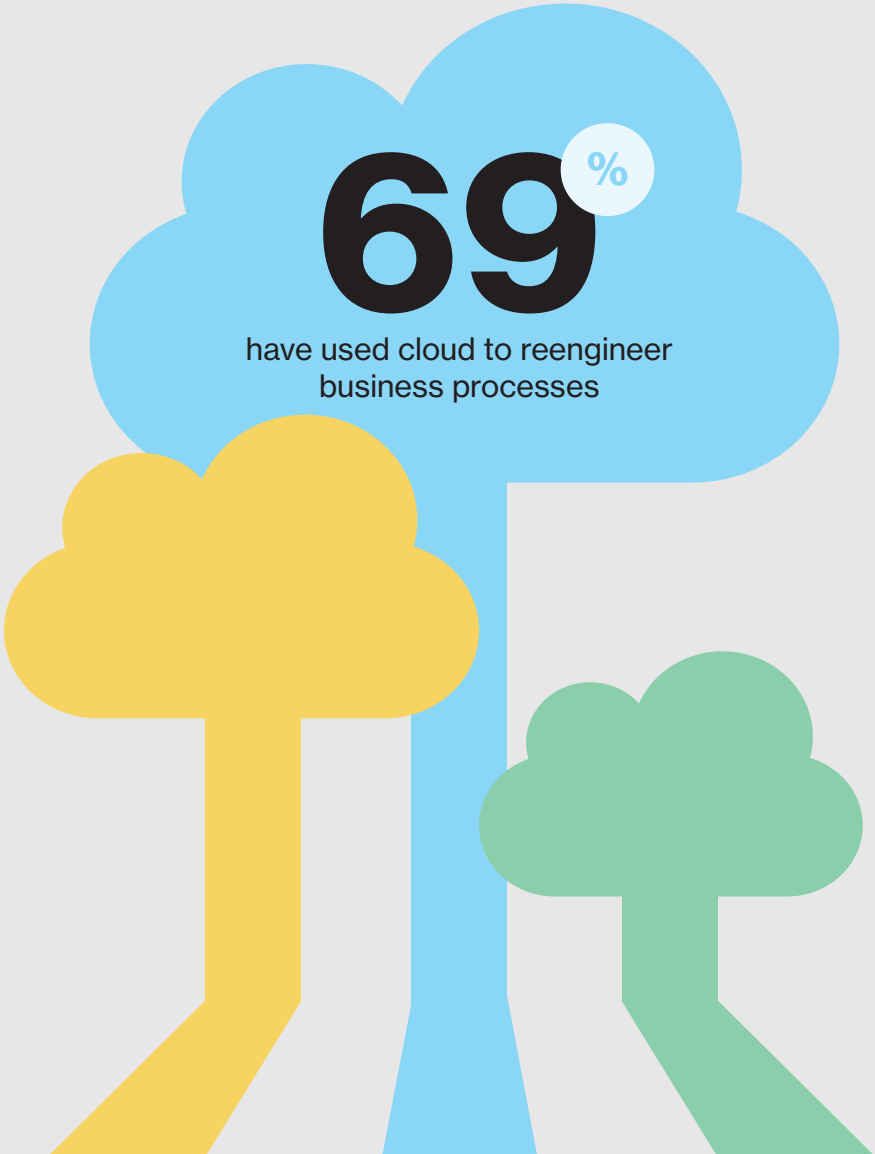
1. TAX incentives for setting data centre in India similar to STPI.
2. Put data privacy law in place in addition to fundamental right to privacy.
3. Retrospective implementation of law/regulations to avoided in letter and spirit.

**********

# State of the Market: Enterprise Cloud 2016.

**From adoption to transformation.**

verizon



The evolution continues. Last year the news was that cloud was being used for mission-critical workloads. Cloud's now firmly established as a reliable enterprise workhorse, and what's most interesting is how it's driving transformation. Organizations are using cloud to create new customer experiences, reengineer their business processes and find new opportunities to grow.

## Sources

In writing this year's report, we've drawn on multiple data sources:

- Verizon reports: including last year's *State of the Market: Enterprise Cloud 2014* report.
- Verizon customer survey: survey of Verizon's enterprise-level cloud customers (October 2015).
- Verizon-commissioned research: Harvard Business Review Analytic Services report *Cloud: Driving a faster, more connected business*, commissioned by Verizon (2015).
- Third-party research: studies from Forrester Consulting, Gartner and IDC to add additional perspective to our findings.

## Contents

# From adoption to transformation.

In the three years we've been producing this report, we've seen cloud go from a newcomer to part of the established order. But despite the maturity of cloud, the market is still developing and most organizations are still finding new and exciting ways to take advantage of it.

In last year's enterprise cloud report[1] we talked about how cloud was redefining the role of IT. That's proceeded apace. In many organizations the IT function is now much more closely aligned with the lines of business (LOBs) and is adept at managing a portfolio of cloud providers.

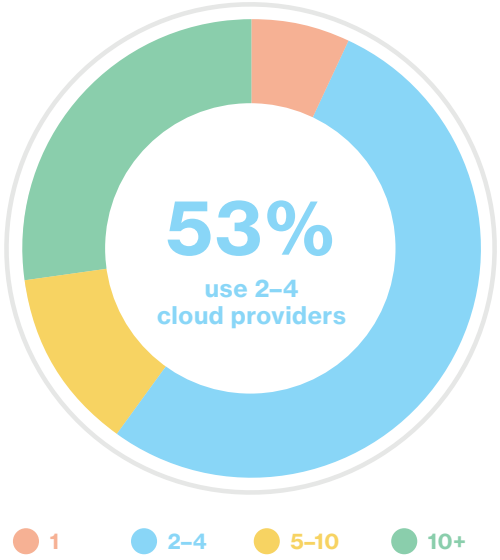



Figure 1: Number of cloud providers[2]

It's not just IT functions that are changing, cloud providers are too. Sophisticated new services and powerful new tools are making it possible for even the largest, most ambitious organizations to put their whole infrastructure in the cloud and transform their business.

Companies are combining public, private and on-premises infrastructure to create highly sophisticated, customized environments. These environments can provide the ideal mix of performance and flexibility. This can enable even the most established organization to do things in new ways, and disrupt even the most entrenched industry.

**69%**

say that cloud has enabled them to significantly reengineer one or more business processes[2].

We've seen lots of change, but there's more to come. In this paper we'll discuss:

- How cloud use is growing more sophisticated.
- The importance of cloud in digital transformation.
- The three different personas that are emerging.
- Ways in which cloud is being incorporated into IT strategic decision-making.
- How organizations are looking to managed services to make the most of cloud.

**So what's the state of cloud today? Read on.**

In just a couple of years, we believe that over half of all workloads — across organizations of all kinds — will be running in the cloud.

# Everybody's doing it.

Another year, another plethora of cloud adoption reports saying that cloud adoption is reaching 100%. By that we mean almost all companies are using cloud, not that all organizations are using cloud for everything.

### Proportion of workloads in the cloud

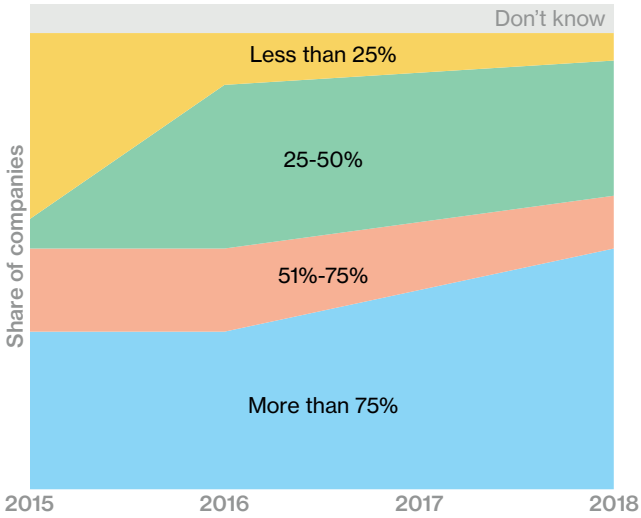



Figure 2: Shifting share of workloads in the cloud[2]

In last year's report[1] we found that cloud spend had grown 38% year-on-year. That phenomenal growth continues, with 84% of companies saying that their use of cloud has grown in the last year[2].

**84%**

of respondents say their use of cloud increased in the past year[3].

Around half of companies say that they will be using cloud for at least 75% of their workloads by 2018. In just a couple of years, we believe that significantly over half of all workloads – across companies of all kinds – will be running in the cloud.

## Using cloud isn't enough anymore

As cloud increasingly becomes the norm, the edge it gives a company is falling. It still has a major role to play in delivering competitive advantage, but using cloud is now just table stakes.

### Competitive advantage of using cloud

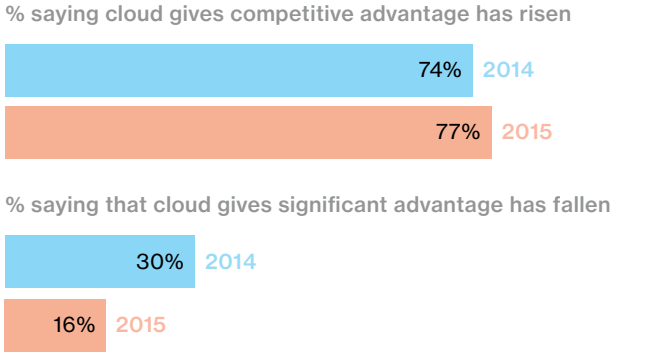



Figure 3: Competitive advantage of using cloud, 2015 versus 2014[3]

It's not enough to think "cloud first". To derive significant competitive advantage from cloud you need to think how you can leverage it to enable digital transformation, change how you do business, and disrupt your market.

### Has cloud enabled you to adapt business model?

(for instance, moving to usage-based pricing)

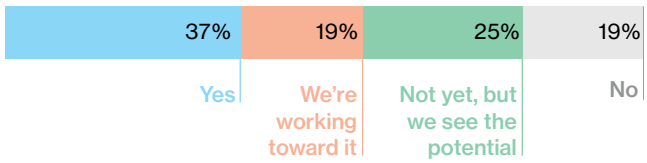



Figure 4: Organizations using cloud to adapt their business model[2]

Our research shows that more than a third of organizations have already adapted their business model using cloud – for example, creating new customer experiences or radically changing their cost base. A further fifth are in the process of doing so[2].

**Is your strategy fit for the future?**

Which persona fits you best?

# Strategies are diverging.

As the use of cloud has matured, the ways in which companies are using it have diverged. While every company is different, they fall into three personas: the skeptics, the natives and the pragmatists.

## The skeptics

It's now widely recognized that technology is key to competitiveness, even survival. And so it's unsurprising that today it's very unusual for us to find an organization that hasn't adopted cloud to some degree. Only 6% of respondents in our survey said they think their company will have less than 25% of workloads in the cloud by 2018, shown in Figure 2.

It's not that these companies – we call them skeptics – don't see the potential benefits of cloud, it's that they are yet to be fully convinced. Companies in this group aren't rejectors, they almost certainly use SaaS, and probably lease hardware and software stacks from vendors. While this doesn't give them demand-based pricing, it does give them some insulation from upfront capital costs.

Skeptics' reluctance is often due to corporate attitude toward risk management, governance, or capital investment. Some industries, like financial services, are home to more skeptics than others. As cloud becomes more established and skeptics see what their competitors are able to do with cloud, their numbers are dwindling.

## The natives

It's not just the unicorns – those highly distinctive businesses like Uber and Spotify, often cited as examples – many businesses are now cloud-first or even cloud-only. We call these companies the cloud natives.

You don't have to be small or a start-up to be a cloud native. With everything from spreadsheet to enterprise resource planning (ERP), customer relationship management (CRM) and payroll software available in the cloud on a subscription basis, many companies are choosing to buy services rather than servers.

## The pragmatists

The skeptics and natives form the ends of a wide spectrum. The majority of organizations are taking a measured approach, striving to create an enterprise-class infrastructure using standard components from cloud providers tied together using APIs and orchestration services. We call these companies the pragmatists.

> Typically these companies have a thorough understanding of what's involved in a cloud project and what options are available.

Even when faced with an extremely demanding workload with complex requirements, they will work with specialist enterprise service providers to build the infrastructure they need. This might include sophisticated load-balancing and acceleration, and highly resilient, ultra-high bandwidth connections between systems.

In a sense, these organizations are the true believers. Even though they have large estates and complex legacy applications, they are so convinced by the benefits of the cloud approach that they are rewriting the rulebook.

This model, hybrid IT, brings together cloud, both public and private, with on-premises and colo. It also recognizes the importance of the network. Tying all this together can be challenging. Many pragmatists have turned to managed services providers to help them.

The companies leading the way in this group use a sophisticated scoring system to assess each workload on characteristics like sensitivity of data stored, availability requirements, and elasticity required. Some have even automated this process so that they can spin up an appropriate environment with little manual involvement.

Some early pragmatists relied heavily on vendor-specific cloud features, making it hard to move systems as needs changed and new options emerged. Because of that, pragmatists are focusing on how to avoid vendor lock-in while increasing automation.

Most companies need a mix of different types of cloud to provide the value, manageability and security they require.

# Models are changing.

## Private cloud is becoming less exclusive

> We see companies increasingly turning to private cloud and believe that in the future public cloud will only be used in very specific circumstances.

One of the biggest changes we're seeing in the cloud market is a dramatic fall in the barriers to entry of private cloud. This is largely being driven by advances in technology. Lower starting costs mean that private cloud is no longer only suitable for those with huge budgets – even a relatively small number of servers can be economically viable as a private cloud. And this narrowing of the price difference between public and private cloud is changing the value equation.

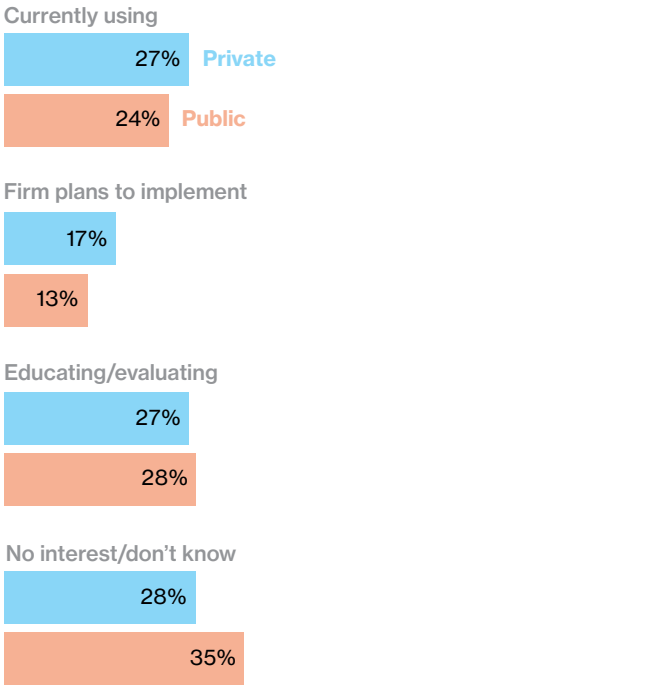



Figure 5: Enterprise expectations of cloud adoption[4]

In the past, the approach taken by many companies roughly followed a similar model: public for non-sensitive workloads; private cloud for more sensitive stuff; and traditional on-premises for difficult-to-move and highly sensitive workloads. Because the cost of private cloud is falling, it now makes sense for many companies to move more of their workloads to private cloud.

There will always be a place for public cloud, especially for workloads that need lots of elasticity but perhaps not so much in the way of risk management and governance. Many websites (but not e-commerce) and testing projects would fall into this category.

But with the cost difference falling, the additional reassurance offered by private cloud is very appealing. We see companies' reliance on public cloud declining (see Figure 5), and believe that in the future it will only be used for a narrow set of workloads.

Likewise, at the difficult-to-move (whether that's due to performance, security or refactoring concerns) end of the spectrum, the cost benefit of moving from legacy environments is now even more compelling. So for many applications destined to be sunset – perhaps five years or more in the future – the cost-benefit analysis now favors an extended life in the cloud.

> Financial benefits (outside of potential cost savings) are significant: 40% say it has increased revenue and 36% say it has increased profit margins[3].

We should stress here that the benefits aren't just financial, they also include keeping users happier, improving risk management, and enabling digital transformation. As we all know, legacy systems are one of the biggest obstacles to system integration and innovation and cloud can help alleviate this.

## Hybrid cloud is now mainstream

Advances in technology are changing the cost-benefit equation and making it easier for companies to build more powerful environments in the cloud, enabling them to move more workloads and transform more processes.

It's been suggested that hybrid cloud – the use of a mix of models, including on-premises and public and private cloud – will become mainstream within five years. We think that it already is, especially for large organizations.

There are already services that enable companies to create a sophisticated environment made up of multiple clouds from multiple providers, but make it look like a seamless part of the enterprise infrastructure.

Many companies still rely on core systems built on legacy technologies that can't be moved to the cloud and which they aren't ready to refactor or replace. This can hold back transformation efforts, like improving the customer experience. With hybrid IT, these systems could be physically colocated in the same place as a private cloud, creating a reliable, high-performance solution.

**75%**

According to a recent survey by Cloud Cruiser, three quarters of companies said that they planned to include hybrid cloud as part of their strategy[5].

Hybrid deployments can be complex to build and maintain. While the technology is already mainstream, it's still a relatively new area and there's a lack of people with the necessary skills and experience.

Many companies are turning to managed service providers to help build and manage the environment they want. Taking this approach can help overcome the challenges with moving to cloud, deliver significant cost and business-agility benefits, and reduce the risk of making the wrong technology decisions.

**Around half of companies now use hybrid cloud, or can easily move workloads between clouds**


Figure 6: The use of mixed cloud environments[4]

Cloud is now an integral part of many companies' IT decision-making processes.

# It's business as usual.

## It's prime time

Organizations aren't just using more cloud, they are using it for applications that are more demanding and more important to everyday operations and performance. This often includes multiple mission-critical applications.

### Do you use cloud for mission-critical workloads?

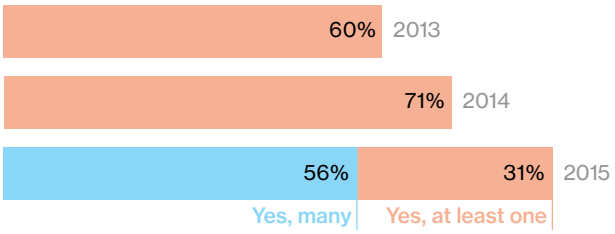



Figure 7: Companies with mission-critical workloads in the cloud[2]

For the types of workloads that organizations put in the cloud from early on – like web apps and dev/test – cloud is now dominant. But cloud is rapidly gaining ground even in mission-critical areas – over a third of companies have at least half their ERP workloads in the cloud.

### Share of workloads in the cloud

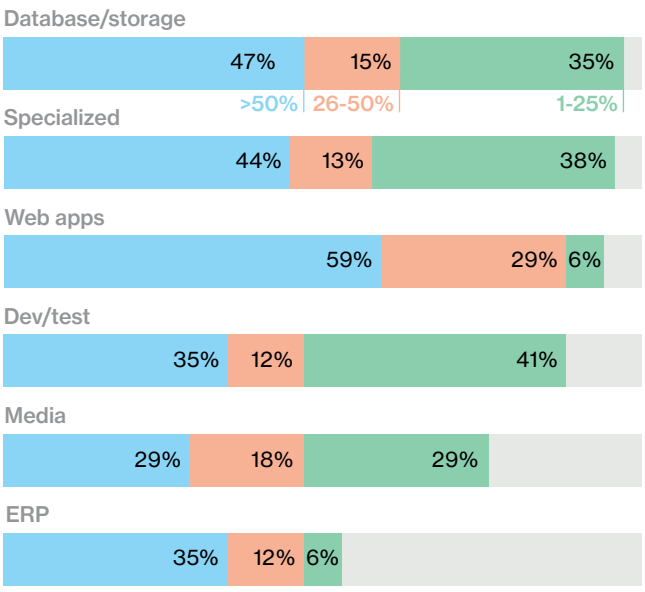



Figure 8: Workloads in the cloud by application type[2]

## It's no longer seen as a "project"

A lot of organizations have completed their first wave of "cloud migration" projects. These projects actively sought workloads to move to the cloud and picked up all the stuff that was easy to move.

But cloud is now seen as just as reliable and secure as traditional delivery models – if not more so. And many companies are considering it alongside on-premises and other delivery options when provisioning a new app or performing a review of their current portfolio.

### What's the availability/reliability of your cloud environment compared to your own on-premises infrastructure?

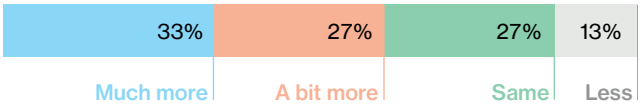



Figure 9: Reliability of cloud versus on-premises[2]

### How secure is your cloud environment compared to your on-premises infrastructure?

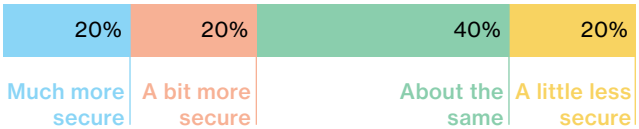



Figure 10: Security: cloud versus on-premises[2]

Some organizations are now targeting specific groups of apps for migration, often because they are difficult to manage or becoming a roadblock to transformation. We're also seeing more and more workloads moved as part of routine application portfolio management.

**68%**

say they must invest in cloud/ SaaS to achieve business priorities[6].

## It's chosen for strategic reasons

Application portfolio reviews consider the value delivered by each application versus its cost – including maintenance and support. While cost was an early differentiator for cloud, increasingly organizations are choosing cloud for the value it can add, not how much it can save them.

### Main reasons for moving mission-critical workloads into the cloud

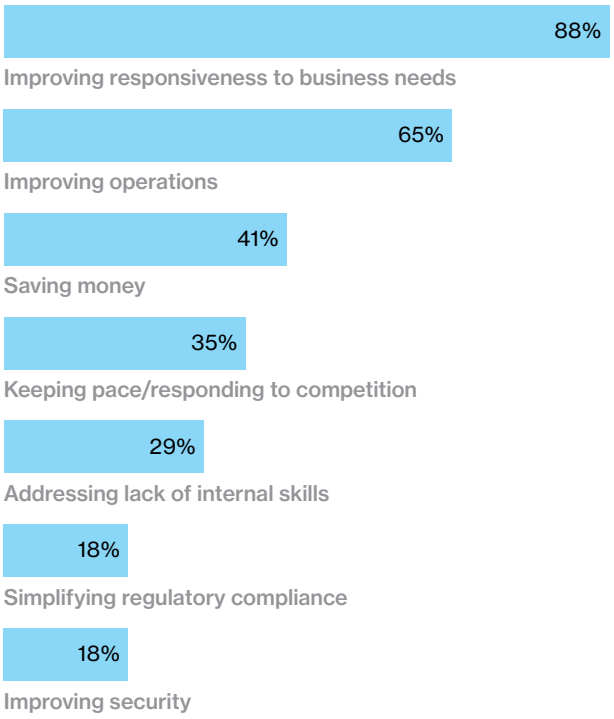



Figure 11: Reasons for migrating mission-critical workloads[2]

But the capabilities and economics of cloud are changing so quickly that organizations must review their decisions more frequently. Where in the past decisions about core systems might have looked 20 years ahead, today decisions made just a year ago could be no longer valid. Failure to revisit plans doesn't just risk overspending on IT, but could mean being outmaneuvered by competitors and losing market share.

## It's many companies' first choice

A growing number of organizations – the US government was one of the earliest – have made cloud their preferred choice. It's not just natives, many pragmatists are now thinking "cloud first".

This reflects the fact that not only are the economics favorable, but cloud enables so many of the other things that companies are trying to achieve.

**83%**

say that their company sees IT as "an opportunity to differentiate/ disrupt and gain market share"[2].

Whether it's developing internet of things services, increasing use of mobility or creating new customer experiences, cloud is often an important enabler. Bringing services together in the cloud can help organizations integrate systems and data, accelerate innovation and align business and IT strategies.

**55%**

say they need to invest in alignment of business and IT strategy to meet their 2015 business priorities[6].

Just because cloud is no longer new doesn't mean it doesn't present challenges. There's plenty to do to make the most of the opportunities.

# Recommendations.

## Keep projects short

While it's important to take a strategic approach to cloud, with structured programs and robust measurement, it's important to keep projects short.

> Many cloud migration projects can be completed quickly and these are the most likely to be successful.

We've found that six months is a good upper limit on the length of a project. This helps maintain momentum and limits the impact of technology changes.

## Don't try to do it alone

Cloud is a broad field and a rapidly moving one. Keeping abreast of the changes in technology is no easy feat. It's not just hard to recruit and train the right people, it's difficult to know what skills you'll need in a year's time.

Many companies lack sufficient experience with cloud projects, especially those involving mission-critical applications and major transformation. And while standards and frameworks are evolving, these are only part of the answer.

> In the absence of any agreed standard, many US state and local government bodies are adopting the federal government's FedRAMP framework to assess cloud services.

Managed service providers can supply specialist skills and knowledge, augment internal capacity, and free up the internal team to focus on governance and monitoring how well the cloud platform aligns to business needs.

## Improve transparency

The concept of shadow IT still comes up in many articles on cloud. But in our experience it's more of a media fascination than a reality. While the LOBs have more technical expertise than before, they still rely on IT.

Despite the advent of cloud, managing enterprise infrastructure remains a highly specialized task and even IT departments are struggling to attract and retain the right talent. Most organizations believe that achieving digital transformation requires a well-thought-out, companywide approach — not mavericks with credit cards.

> Another interesting data point revealed that 44% of the respondents do not have any means to employ chargeback or showback for their delivery of IT services, but 56% indicated that they were planning to provide service cost transparency to their businesses[5].

Most IT functions have adapted to meet the demand to be more responsive and flexible, but there's still room for improvement. Studies suggest that IT budgets are only growing slowly, if at all, and most of that money is still being spent on keeping the lights on.

The provisioning and movement of environments will eventually be highly automated based on business rules. Until then, the IT function must serve as a center of excellence for scoping and management. Improving reporting on performance and internal recharging will help IT demonstrate the value that it's adding and get the money it needs to fund transformation.

## Continually reassess security

Managing risk remains a "go to" topic when discussing cloud. Few articles fail to highlight the perceived dangers. But in the last two surveys that we've undertaken, fewer than 5% of companies had experienced a significant data breach that was directly attributable to a cloud-based service – and that includes SaaS applications[2].

As cloud became more pervasive within organizations, IT had to step in and make sure that it was properly managed from a policy, control and compliance standpoint. The result has been a decline in shadow IT projects, clearer definitions of expectations and greater service-provider transparency. So now when we ask about cloud, most companies say that their cloud environment is as secure, if not more secure, than their traditional infrastructure.

In the past, studies have shown that many companies keep paying for security services that have been shown to be ineffective – a bit like sticking to your lottery numbers. The shift to cloud forces companies to reassess the focus of their security and governance spend, and this can lead to greater effectiveness and better value for money.

Reporting has a key role to play. When assessing cloud providers, ask them about their reporting capabilities. Choose one that's able to provide extremely granular and reliable information on demand and performance, consistently across applications and functions. As well as providing valuable inputs for planning, this information can help you keep reassessing your security needs.

Some vendors have launched specialized solutions tailored to specific security and compliance needs. Consider options, like PCI-DSS- or HIPAA-friendly services, to accelerate solution development and reduce the burden of managing governance and compliance.

## Don't forget the network

IT and the LOBs, and even analysts, agree that connectivity is critical to the success of cloud projects.

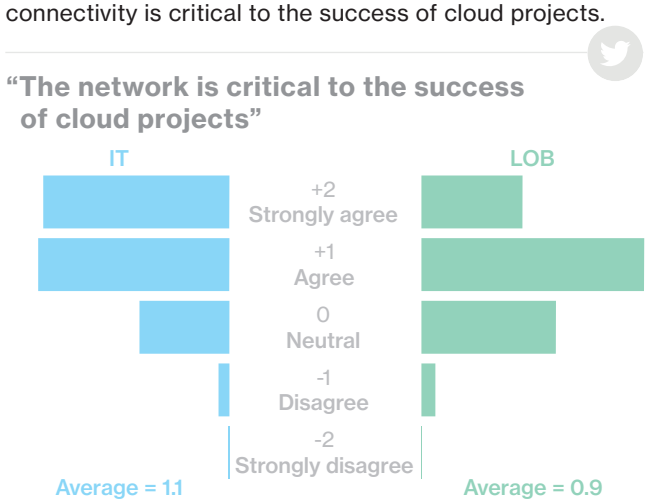



Figure 12: Agreement with the statement "the network is critical to the success of cloud projects", split of respondents[6]

As more companies have come to rely on cloud services for mission-critical workloads, the importance of connectivity has grown. Many companies have already switched to dedicated cloud connection services to improve performance and reliability.

> Through 2015, at least 50% of cloud deployments will suffer from business-impacting performance issues, requiring extensive network redesign to address them[7].

Software-defined networking (SDN), promises to bring many of the same benefits to networks that cloud has to hosting. While SDN is still in its infancy, it's something you should take into account when making network decisions.

**To find out more about how our managed cloud services can help you move more complex workloads, create an effective hybrid IT environment, and allow you to focus on innovation, not infrastructure, visit:**

**verizonenterprise.com/cloudreport2016**

References

1 State of the Market: Enterprise Cloud 2014, Verizon, October 2014.

2 Verizon customer survey: survey of Verizon's enterprise-level cloud customers, October 2015.

3 "Cloud: Driving a faster, more connected business", a 2015 Harvard Business Review Analytic Services report, sponsored by Verizon.

4 IDC IView, sponsored by Cisco, Don't Get Left Behind: The Business Benefits of Achieving Greater Cloud Adoption, August 2015.

5 Cloud Cruiser, Survey of AWS re:Invent Conference Attendees indicates 75% plan on operating a Hybrid cloud, December 2014.

6 A commissioned study conducted by Forrester Consulting on behalf of Verizon, February 2015.

7 Gartner Presentation, Cloud, SDN and the Evolution of Enterprise Networks, October 2014.

**verizonenterprise.com**

ECIPE OCCASIONAL PAPER • No. 3/2014

# THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY

Matthias Bauer
Hosuk Lee-Makiyama
Erik van der Marel
Bert Verschelde

EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY
ECIPE

www.ecipe.org

info@ecipe.org Rue Belliard 4-6, 1040 Brussels, Belgium Phone +32 (0)2 289 1350

*"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind."*

—Lord Kelvin

## SUMMARY


- This paper aims to quantify the losses that result from data localisation requirements and related data privacy and security laws that discriminate against foreign suppliers of data, and downstream goods and services providers, using GTAP8. The study looks at the effects of recently proposed or enacted legislation in seven jurisdictions, namely Brazil, China, the European Union (EU), India, Indonesia, South Korea and Vietnam.
- Access to foreign markets and globalised supply chains are the major sources of growth, jobs and new investments – in particular for developing economies. Manufacturing and exports are also dependent on having access to a broad range of services at competitive prices, which depend on secure and efficient access to data. Data localisation potentially affects any business that uses the internet to produce, deliver, and receive payments for their work, or to pay their salaries and taxes.
- The impact of recently proposed or enacted legislation on GDP is substantial in all seven countries: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%) and Vietnam (-1.7%). These changes significantly affect post-crisis economic recovery and can undo the productivity increases from major trade agreements, while economic growth is often instrumental to social stability.
- If these countries would also introduce economy-wide data localisation requirements that apply across all sectors of the economy, GDP losses would be even higher: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%).
- The impact on overall domestic **investments** is also considerable: Brazil (-4.2%), China (-1.8%), the EU (-3.9%), India (-1.4%), Indonesia (-2.3%), Korea (-0.5%) and Vietnam (-3.1). **Exports** of China and Indonesia also decrease by -1.7% as a consequence of direct loss of competitiveness.
- **Welfare losses** (expressed as actual economic losses by the citizens) amount to up to $63 bn for China and $193 bn for the EU. For India, the **loss per worker** is equivalent to 11% of the average month salary, and almost 13 percent in China and around 20% in Korea and Brazil.
- The findings show that the negative impact of disrupting cross-border data flows should not be ignored. The globalised economy has made unilateral trade restrictions a counterproductive strategy that puts the country at a relative loss to others, with no possibilities to mitigate the negative impact in the long run. Forced localisation is often the product of poor or one-sided economic analysis, with the surreptitious objective of keeping foreign competitors out. Any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy.

## INTRODUCTION

Over the past few years, there has been a widespread proliferation of regulatory restrictions of the internet, in particular for commercial use. Whereas governments' earlier endeavours to increase control over the internet had the implicit aim of keeping information outside state borders, this new breed of regulation aims at keeping data in. With the pretext of increasing online security and privacy, some governments are requiring mandatory storage of critical data on servers physically located inside the country, i.e. data localisation. Also, some data protection and security laws create barriers to cross-border data transfers to such an extent that they are effectively data localisation requirements.

The belief that forcing personal information, emails and other forms of data from leaving the country would prevent foreign surveillance or protect citizens' online privacy is flawed in several ways. First, many of the recent legislative proposals pre-date the surveillance revelations, and are not designed for addressing these issues. Second, information security is not a function of where data is physically stored or processed. Threats are often domestic, while storing information in one physical location could increase vulnerability. Thirdly, data localisation is not only ineffective against foreign surveillance, it enables governments to surveil on their own citizens. Moreover, users and business do not access data across borders with the purpose of evading domestic laws, while legal obligations do not always depend on where a server is physically placed.

As a result, data localisation, or discriminatory privacy and security laws to similar effect, has spawned severe protest from advocates for open internet and the global trading system. Forced localisation is often the product of poor or one-sided economic analysis, with the surreptitious objective of keeping foreign competitors out, or creating a handful of new jobs in e-commerce, data centres or consultancies. However, any job gains as a result of data localisation are minuscule compared to losses in terms of jobs and output in other parts of the economy.

Access to foreign markets through trade liberalisation and globalised supply chains are major sources of growth, jobs and new investments – in particular for developing economies. Given the nature of today's globally interconnected economy, poorly designed national policies that increase data processing costs have a severe economic impact as many sectors of the economy rely on digitally supplied services and goods. Manufacturing and exports sectors are also dependent on having access to a broad range of services at competitive prices – such as logistics, retail distribution, finance or professional services – which in turn are heavily dependent on secure, cost-efficient and realtime access to data across borders. When data must be confined within a country, it does not merely affect social networks and email services, but potentially any business that uses the internet to produce, deliver, and receive payments for their work, or to pay their salaries and taxes.

This paper aims to quantify the economic losses that result from data localisation requirements and related data privacy and security laws that discriminate against foreign suppliers of data. It does so by using a computable general equilibrium model (CGE) called GTAP8 (see Annex II), which is a well-acknowledged methodology that is frequently used for trade and economic impact analyses by academia and policymakers worldwide. The study looks at the effects of the recently proposed or enacted legislation in seven jurisdictions, namely Brazil, China, the European Union (EU), India, Indonesia, South Korea and Vietnam. Some of these countries have conducted quantitative impact studies (notably the EU) measuring institutional or firm-level costs.[1] Yet, no public study by a market regulator has investigated

the effects on exports, gross domestic product (GDP) and consumer welfare as a result from proposed data localisation requirements or privacy laws.

## OVERVIEW OF RELEVANT INTERNET AND PRIVACY REGULATIONS

The analysis looks at a number of recently introduced or proposed measures with respect to data localisation by conducting a survey in each of the aforementioned countries' jurisdictions. The measures are assumed to alter the costs of engaging in commercial activities in the selected countries (a brief description of all measures in each country can be found in Annex I). The way in which these primarily privacy and security related measures operate is of principal importance for accurate data modelling. For instance, data localisation requirements are effectively disruptive bans of data processing and hence the foreign provision of that service into the domestic territory. The ban can be introduced economy-wide (e.g. China, Vietnam), or selectively to a particular sector (e.g. only financial services in Korea).

Besides data localisation, a number of administrative regulatory barriers could be introduced through additional legal obligations that increase compliance costs, such as stricter consent requirements, a right to review personal information held by firms, the requirement to notify a market regulator and/or data subjects in case of potential security breaches. Some measures are institutional such as the requirement to appoint a data privacy officer (DPO) within the organisation; while others increase business risks by introducing sanctions for non-compliance (in many cases with ambiguous laws), or a government's right to access a business proprietor's or its clients' data.

Overall, compliance with these measures increases the operational expenditure of firms which raises domestic prices and non-tariff barriers (NTB) on imports. Therefore, in order to measure the actual or potential costs of introducing these measures, for this paper we have estimated the costs of all data localisation measures using two different scenarios:

- Scenario 1, which is based on the actual proposed regulations as defined in Table 1, including data localisation in each country as per today.
- Scenario 2, which is based on the actual proposed regulations, but with the addition of a data localisation requirement applied to all sectors in each country.

**TABLE 1: OVERVIEW OF REQUIREMENTS IN LEGISLATIVE PACKAGES**

| | Brazil | China | EU28 | India | Indonesia | Korea | Vietnam |
|---|---|---|---|---|---|---|---|
| Data localisation requirement | No | Yes | No | Partial | Yes | Partial | Yes |
| Consent required for data collection | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Consent required for transfer to third parties | Yes | Yes | No | Yes | No | Yes | No |
| Right to review | No | No | Yes | Yes | Yes | Yes | No |
| Right to be forgotten | Yes | Yes | Yes | No | No | Yes | Yes |
| Breach notification | No | Yes | Yes | No | Yes | Yes | No |
| Impact assessment | No | Yes | Yes | No | No | No | No |
| Data privacy officers | No | No | Yes | No | No | Yes | No |
| Sanctions for non-compliance | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Government access required | Yes | No | No | Yes | No | No | Yes |
| Data retention requirement | Yes | No | No | Yes | No | No | Yes |

## CONCEPTUAL MODELLING

The scenarios are calculated using several economic shocks caused by data restrictions. If new regulations restrict businesses and individuals from using data in a reasonable manner – prices of any good or service that uses data in its production would also increase. For example, the input costs for a logistics company would increase as they can no longer process data on its customers or shipments using their existing IT suppliers or infrastructure, or are faced with some compliance costs for doing so. This new cost is passed on to its customers – who may be manufacturers, exporters and consumers. Thus, increased regulation leads firstly to domestic productivity losses for various sectors of the economy. Secondly, it creates an additional trade barrier against data processing and internet services, or any service (to a lesser extent also goods) that depends on the use of data for delivery. Thirdly, as the competitiveness of the economy changes, investments (both domestic and foreign) will be affected. Finally, the effectiveness of R&D is affected to the extent that product development depend on customer and market data to compete in the market place.

The first shock, which measures the effect on productivity, is created using a so-called augmented product market regulatory (PMR) index for all regulatory barriers on data, including data localisation, to calculate domestic price increases or total factor productivity (TFP) losses.[2] It sets out what domestic companies will have to pay additionally for sourcing domestic data services by first estimating the general effect of administrative burdens in data processing services on prices and TFP in each sector of the economy. Data processing services is an important input for production – and by using existing indexes from the OECD measuring administrative barriers in services over time, we evaluate the extent to which these administrative barriers in data services affect other parts of the economy through the use of data services. For example, the telecommunications sector is very data intensive (with 31% of its inputs being data-related) and should be more heavily affected by regulation; similarly, data processing is 5 to 7% of the total inputs used by business/ICT and financial services.[3]

The index is then raised based on the regulatory barriers as given in Table 1 for each country. Not all of these measures are equally restrictive, and their relative importance is therefore weighted according to their relative cost impact.[4] By benchmarking the resulting index against the estimate prior to the legislation and data processing intensities for all sectors, we compute the price and TFP changes for all sectors in each country as a result of data localisation and administrative barriers.

The second methodology computes cost differences between countries as a result of data localisation requirements in each of the countries. Two types of data are primarily used – namely the Data Centre Risk Index,[5] and an empiric observation of cost differences.[6] The first source ranks countries according to a number of risk factors that affect the costs of operating a data centre – a ranking that closely follows the general cost structure across countries of setting up a centre as a consequence of data localisation measures. The observations of actual costs are broadly in line and thereby confirm the Risk Index.

These costs are up-front trade costs each firm will need to incur when investing in and exporting to one of our selected countries (see Annex II). These trade costs are allocated across all sectors in each economy based on the intensity with which each sector uses data services. The final numbers are interpreted as the additional costs a firm will need to pay for using data services when entering one of the countries in which data localisation laws are implemented.

The third shock occurs on investment, which forms a major driver for economic growth for developing countries in particular. However, as the regulatory environment imposes more

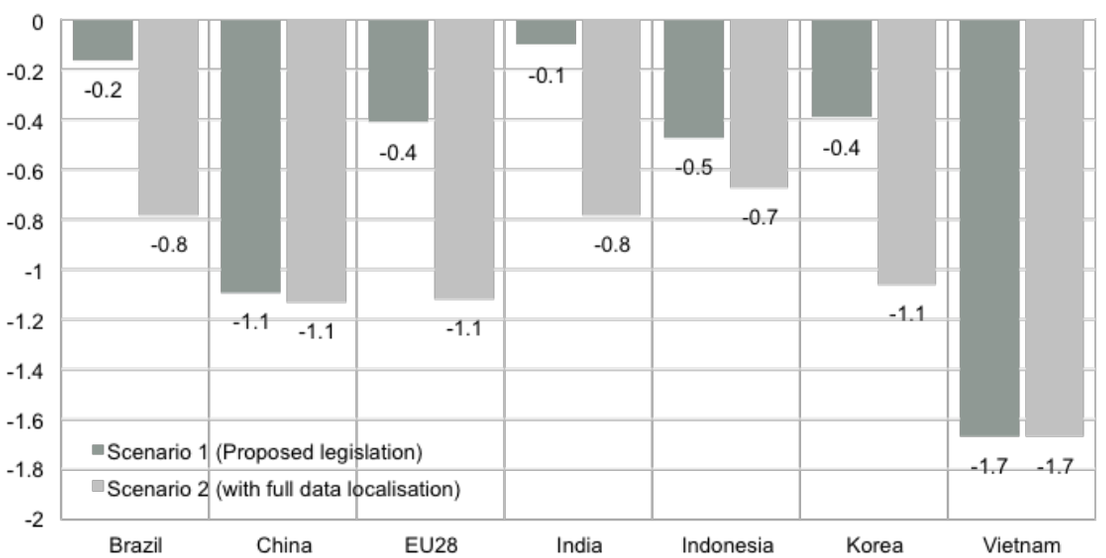
market limitations, investments made by both domestic and foreign entities will decrease. In GTAP8 this is introduced as a change in rate of return on investments (see Annex II). Furthermore, a final shock occurs as an additional effect on the return on investment, which is derived from research and development. A survey by Xu, Zhu, Gibbs (2004) provides the share of firms in developed and developing countries respectively that uses online sales, advertising or electronic data interchanges (EDI).7 These numbers are also consistent with industry reports on the share of firms that uses CRM (customer relationship management) applications for data mining of their customers.8 The relation between R&D expenditure and return is given by several studies (notably Hall, Foray, Mairesse, 2009; Ortega, Argilés, 2009, Rogers, 2009), based on empirical evidence.

## THE OUTCOME OF THE SIMULATIONS

The outcome of the simulations shows that the impact on economic activity in all economies is considerable. Figure 1 summarizes the results of the two scenarios outlined above. The realistic Scenario 1 naturally gives lower overall outcomes than Scenario 2 except for China, Indonesia and Vietnam where economy-wide data localisation has already been introduced or is being considered (and is hence included already in Scenario 1).

India suffers the lowest GDP effects as a result of our simulations in the realistic scenario 1. However, this would increase drastically if India were to implement a data localisation requirement. Brazil also has relatively low GDP losses (0.2%) based on Scenario 1 but this effect quadruples if data localisation is applied. Both the EU and Korea also report substantial differences between the two scenarios as a result of economy-wide data localisation.

**FIGURE 1: GTAP SIMULATIONS ON GROSS DOMESTIC PRODUCT (GDP) FOR SELECTED COUNTRIES. CHANGES IN %**



Overall, for some countries these losses are rather sizable. In many cases, the effects on GDP are sufficient to eradicate the economic gains produced by most trade agreements they have negotiated or are currently negotiating, e.g. Transatlantic Trade and Investment Partnership (TTIP) or Trans-Pacific Partnership (TPP) – for instance, in the case of Brazil, Vietnam and Korea current growth projections would be dented by at least one-third (figure 2).

The GDP loss in Scenario 1 is sufficient to put the EU back into decline (figure 3) – also, the European Commission projects a GDP growth of one percent in seven years (approx. 0.14% year-on-year) from its European Cloud strategy, whereas data localisation leads to at least 1% decline in just one year for the EU.

**FIGURE 2: PROJECTED GDP GROWTH (2014); ADJUSTED FOR SCENARIO 2 CHANGES IN %**

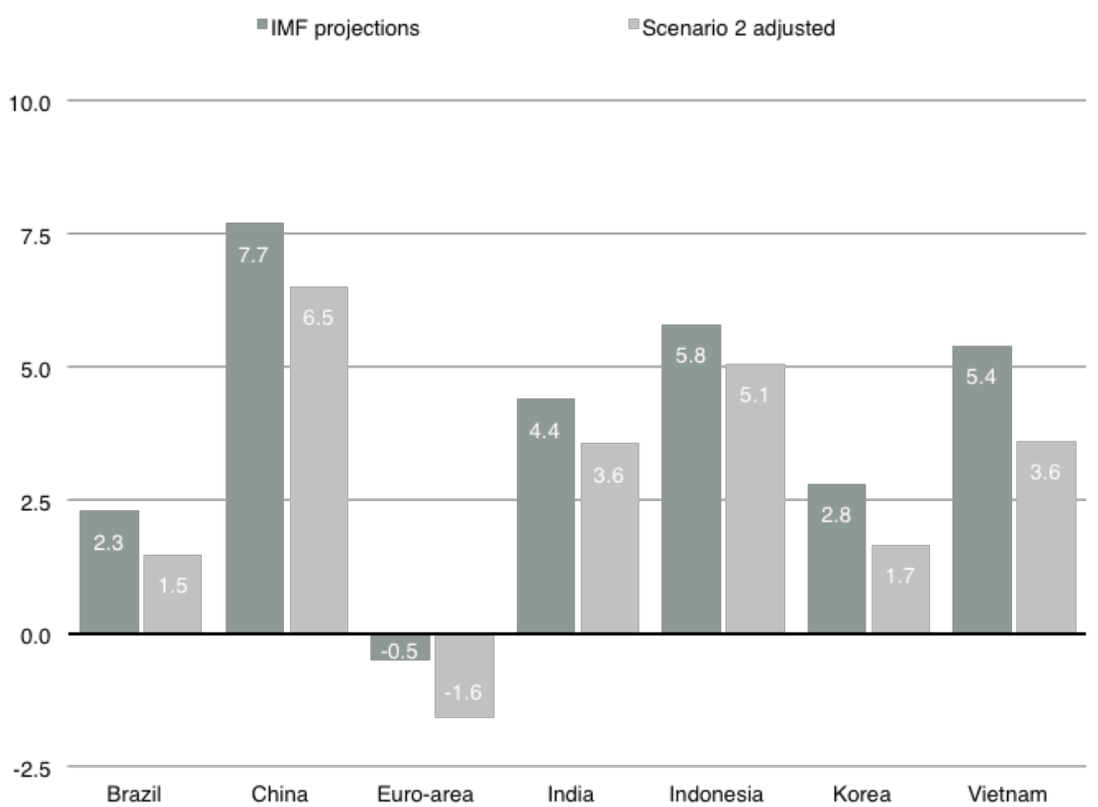
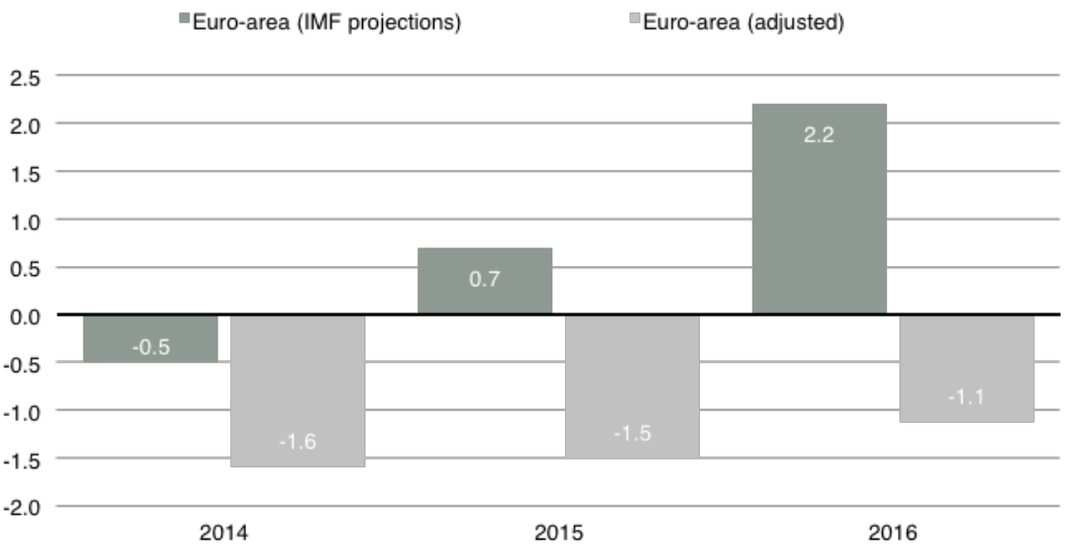


**FIGURE 3: PROJECTED GDP GROWTH FOR THE EURO ZONE ACCUMULATED CHANGES IN % SINCE 2013**




As explained above, the GTAP model also allows for an outcome analysis on investment for each country. Figure 2 sets out the results which show that considerable changes in domestic and foreign investments can be expected as a result of the deteriorated regulatory environment. The figure shows that Brazil and the EU would suffer most from lower investments under both scenarios. One potential reason is that both economies are very investment intensive in those services (and goods) sectors which rely on data services the most. Other countries such as China, India and Indonesia would experience an equal loss in investment under both scenarios albeit still substantial. Korea reports a large difference between both scenarios.

**FIGURE 4: GTAP SIMULATIONS ON INVESTMENTS FOR SELECTED COUNTRIES. CHANGES IN %**

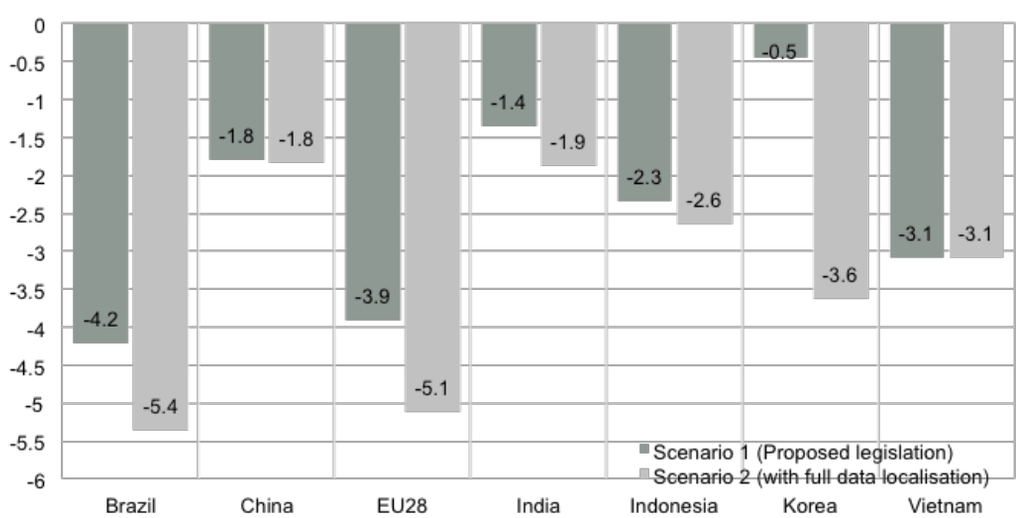
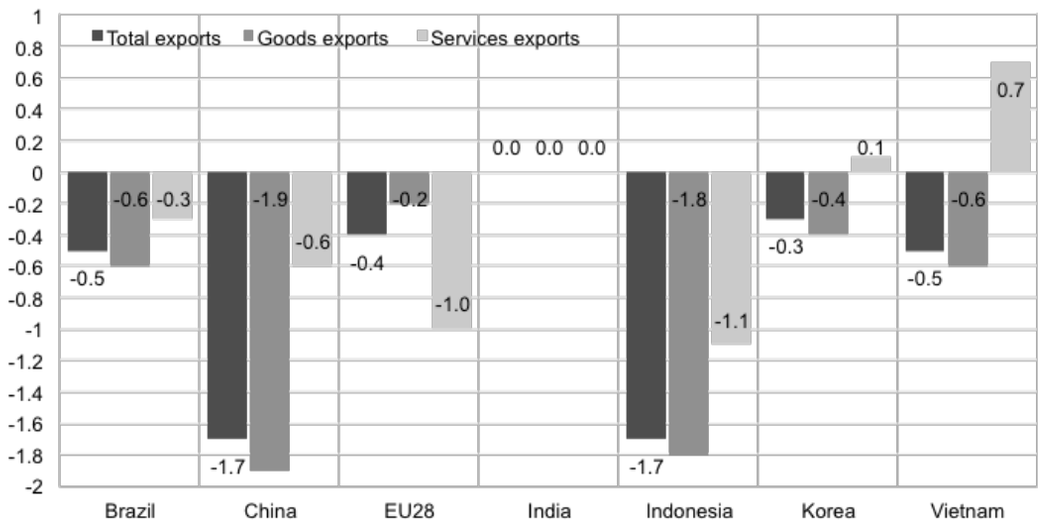


Figure 5 finally sets out the changes for trade, both in terms of total exports, goods exports and services exports. First we note that the exports effects are lower than the investment changes reported in Figure 2. A second interesting issue with regards to the trade effects is that for some countries such as Brazil, China and Indonesia, but also Korea and Vietnam the negative effects on goods exports are greater than for services. This is most likely due to the fact that none of the selected countries are services-driven economies, with the exception of the EU where the services exports losses are greater.

**FIGURE 5: GTAP SIMULATIONS ON EXPORTS FOR SELECTED COUNTRIES. CHANGES IN %**




Overall, the welfare losses that are incurred are mostly derived from higher prices and displaced domestic demand that cannot be met by supply. Table 2 finally sets out the total and per capita nominal costs for each scenario based on our GTAP calculations. One can see that the welfare losses in China (61.6-63.8 bn US$) and the EU (80-193 bn US$) are greatest, followed by Korea (5.3-15.9 bn US$), Brazil (4.7-15 bn US$) and India (3.1-14.5 bn US$)) Both Vietnam and Indonesia are least affected in nominal terms, although this does not mean that their economies would not suffer significantly, in particular noting the changes in GDP and variance in median incomes of some of the countries.

**TABLE 2: WELFARE EFFECTS FROM DATA LOCALISATION AND PRIVACY BARRIERS IN CURRENT US$**

| | Brazil | China | EU28 | India | Indonesia | Korea | Vietnam |
|---|---|---|---|---|---|---|---|
| Scenario 1 | -4.7 bn. | -61.6 bn. | -80 bn. | -3.1 bn. | -2.7 bn. | -5.3 bn. | -1.5 bn. |
| Scenario 2 | -15 bn. | -63.8 bn. | -193 bn. | -14.5 bn. | -3.7 bn. | -15.9 bn. | -1.5 bn. |
| Scenario 1 (per worker) | -48.9 | -80.7 | -333.9 | -6.7 | -24.9 | -218.6 | -31.5 |
| Scenario 2 (per worker) | -156.1 | -83.6 | -805.6 | -31.5 | -34.1 | -655.7 | -31.5 |

Table 2 also gives numbers on the welfare costs of data regulation per worker. This negative effect also varies substantially. Nominal figures for the EU and Korea seem large whereas

those for Vietnam, India and Indonesia seem low. Yet, it should be taken into account that the average worker's salary is much lower in the latter countries. To give an example, using comparable average workers' salaries across countries the negative welfare effect would still cost the Indian worker almost 11 percent of one average month salary. Similarly, for China, this impact would come down to almost 13 percent, and even much higher for Korea and Brazil – around 20 percent for both economies.

## CONCLUSION

Industry and internet advocates have warned against an Internet which is fragmented along national borderlines. Some of them are going as far as calling balkanisation the greatest threat to the Internet today, even greater than censorship.[9] One comprehensive study by Chander and Lê (2014) from the California International Law Centre established that data localisation "threatens the major new advances in information technology – not only cloud computing, but also the promise of big data and the Internet of things".[10] It is not unlikely that future trade agreements will include disciplines against data localisation requirements, as there are often less trade-restrictive measures available to address privacy and security.

However, the more immediate effect of data localisation measures – the impact on economic recovery and growth – is even more dangerous. As this study has shown, this impact is a direct consequence of the complex relations between cross-border data flows, supply chain fragmentation and domestic prices. These are complexities that are generally not understood by policymakers, who are often in the field of security and privacy law, rather than international trade. The findings regarding the effects on GDP, investments and welfare from data localisation requirements and discriminatory privacy and security laws are too considerable to be ignored in policy design. It is also reasonable to assume that SMEs and new firms are the first to be displaced from the market, as they lack resources to adapt to the regulatory changes.

In the current security policy context, many regulators and privacy advocates stress the importance of discretion to tackle problems at a national level (e.g. NetMundial 2014 draft conclusions)[11]. The economic evidence however proves that unilateral trade restrictions are counterproductive in the context of today's interdependent globalized economy. The self-incurred losses make data localisation a policy that unilaterally puts the country at a relative loss to others while the possibilities for offsetting the negative impact through trade agreements or economic stimulus are relatively limited over the long term.

## ANNEX I

Brief overview of proposed and enforced acts reviewed

### *Brazil*

The Brazilian internet law "Marco da Civil" started out its life as a crowdsourced legislative proposal in 2009. While it emphasised the fundamental principles of internet freedom and net neutrality, following revelations that Brazilian entities had been subject to US surveillance, new privacy related amendments were made to the bill, including strict consent requirements for data collection, internet users' right to be forgotten and a clear data localisation provision – the controversial article 12, which was later withdrawn.

### *China*

The existence of a plethora of overlapping data privacy laws has traditionally made compliance a very difficult issue in China. Driven by an increasing number of reports on identity theft and illegal trade in personal data,[12] rather than surveillance concerns, China has however taken steps towards privacy reforms – the 'Resolution relating to Strengthening the Protection of Information on the Internet' of December 2013 includes general rules for internet service providers (ISPs) and other businesses prohibiting the collection of personal data without consent and the illegal transfer or sale of personal information to third parties.[13] In the same year, the Standardisation Administration and the General Administration of Quality Supervision, Inspection, and Quarantine published new national standards that prohibit overseas transfers of data to an entity absent express user consent, government permission, or other explicit legal or regulatory permission. Despite the voluntary character of these guidelines, they serve as "regulatory baseline" for law enforcement and are de facto data localisation laws for all business sectors.[14] The People's Bank of China (PBOC) has also issued a 'Notice to Urge Banking Financial Institutions to Protect Personal Financial Information',[15] which explicitly prohibits off-shore storing, processing or analysis of any personal financial information of Chinese citizens; meanwhile the Ministry of Industry and Information Technology (MIIT) has banned collection of personal data without consent or without 'specific and clear purpose'.[16] 'The Telecommunications and Internet Personal User Data Protection Regulation' also requires regular risk impact assessments to be conducted by data processors.

### *The European Union*

In January 2012, the European Commission proposed a reform of the EU's data protection regime, which is currently based on the 1995 Data Protection Directive. The aim of the new proposal, dubbed the General Data Protection Regulation (GDPR), is to establish a single European-wide data protection law. Aside from simplifying administrative procedures and centralizing supervisory authority, GDPR also introduces strict consent requirements, a right to review, a right to be forgotten, and the obligation for businesses to appoint a data protection officer (DPO) and perform an annual data protection impact assessment (DPIA). If implemented, the GDPR reform could lead to a stoppage of cross-border data flows from the EU to important data processing countries such as the US and India, which are deemed to have adequate data privacy safeguards in place under the EU's current regime.

Aside from GDPR, the Commission has also adopted a strategy for "Unleashing the Potential of Cloud Computing in Europe". The strategy aims to unify rules and standards related to cloud computing within Europe. If these standards will be designed in a way that decreases

the interoperability with other countries' regulatory regimes, this could lead to a de facto data localization.

### *India*

In 2011, the Indian Ministry of Communications and Technology implemented certain provisions of the 2000 Information Technology Act by publishing privacy rules. These Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules introduced a strict consent requirement that only allows for sensitive personal data to be transferred abroad when "necessary" or when the individual's consent has been obtained.[17,18] These rules also introduced the right to access and review personal information that a company holds. The mercantilist intent of the law is clear, as the government of India issued a clarification to emphasise that the rules do not apply to its expanding outsourcing business.[19] The laws have also been amended with a data retention requirement (with duration at the discretion of the government) for intermediaries that so far has not been implemented.

National media in India have reported that the National Security Council Secretariat (NSCS) is considering proposals that incorporate strong elements of data localisation, mandating all email providers to set up local servers, or that "all data generated from within India should be hosted in these India-based servers and this would make them subject to Indian laws." The strategy also includes creating an Indian email service and ensuring Internet traffic data is routed within India as much as possible, including precedents of forced data localisation for selective cases and services, e.g. BlackBerry mail services in 2012.[20]

### *Indonesia*

ata protection is covered by Law No. 11 of 2008 regarding Electronic Information and Transaction (the 'EIT Law') and Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction ('Reg. 82'), which went into force on 15 October 2012. In order to collect and process data, the data controller needs a legitimate reason for collection and the individual's consent.[21] Regulation 82 further requires a broad and undefined group of companies, "electronic systems operators for public service" to set up a data centre and disaster recovery centre in Indonesian territory for the purpose of law enforcement and data protection. The scope of this requirement is unclear however, as electronic systems operators for public service are not clearly defined. Draft Regulation Concerning Registration Procedure of Electronic System Provider' and January 2014 Draft Regulation with Technical Guidelines for Data Centres contain same ambiguity, although a ministry spokesperson was quoted saying: "[the draft] "covers any institution that provides information technology-based services."[22]

### *Korea*

In the Republic of Korea, the Personal Information Protection Act (PIPA) has been in force since 30 September 2011 and covers all sectors. In addition, the sector-specific Act on Promotion of Information and Communication Network Utilisation and Information Protection ('IT Network Act') regulates the collection and use of personal data by IT service providers.[23] Under these acts, every data handler (including businesses, individuals and government agencies) must appoint a data protection officer (DPO), and consent must be obtained both

for the initial collection and processing of personal data and prior to any transfer abroad or to third parties. PIPA gives individuals the right to review and delete personal data that pertain to them and obliges data handlers to notify the data subjects without delay in case of a data breach. If the number of individuals affected exceeds 10,000, the data handler must also notify the relevant authorities. In addition, Korea prohibits the outsourcing of data-processing activities to third parties in the financial services industry. Banks can therefore only process financial information related to Korean customers in-house, either in Korea or abroad.

### *Vietnam*

In 2013, the Vietnamese government issued Decree 72, on Management, Provision, and Use of Internet Services and Information Content Online, which came into effect on September 1st.[24] The Decree's main aim seems to have been to tighten the government's grip on the Internet and limit free expression,[25] with a broad range of prohibitions under article 5 including opposing the state. The Decree requires ISPs to obtain a license and to register with the Ministry of Information and Communications before providing online services, and all organisations establishing 'general websites', social networks and companies providing services across mobile networks are required to establish at least one server inside the country containing the entire history of 'information posting activities on general information websites (...) and sharing on social networks.'

## ANNEX II

### Description of the GTAP8 model

#### *1. The Model*

The model applied in this study is GTAP 8, a computable general equilibrium (CGE) model.[26] The most recent model setting accounts for inter-sectoral linkages between 129 regions while capturing inter-regional trade flows of 57 commodities. The framework thus allows for a general equilibrium analysis of the economic effects (e.g. GDP effects and changes in trade flows) resulting from the regulation of cross-border data flows. In this model, regional production is characterized by constant returns to scale and perfect competition. Private demand is represented by non-homothetic consumer demands. The structure of foreign trade is based on the so-called Armington assumption, which implies imperfect substitutability between domestic and foreign goods.

The most recent GTAP 8 dataset includes national input-output data as well as trade, tariff and demand structures. The model's base data are primarily benchmarked to 2007. Trade data are based on 2004 and 2007 values while the reference year of protection data is 2007 (see Narayanan et al 2012).[27] Like any applied economic model, this model is based on a number of assumptions. In order to account for recent changes in regional macroeconomic variables, the GTAP 8 dataset on the global economy is extrapolated to 2014.

The exogenous variables used for the extrapolation are macroeconomic variables, i.e. the size of GDP, total population, labour force, total factor productivity and capital endowment as provided by the well recognised database of the French research center in international economics (CEPII), which is documented by Fouré et al (2012). We apply the estimates of these macroeconomic data projections in order to calculate the "best estimate" of the global economy in 2014. Preferences and production structures as described by the model's structural parameters have been left unmodified.

The model we use in this study is comparative static. This model does not account for endogenous productivity growth and may thus under-predict welfare effects, economic growth and increases in trade flows that result from the imposition of NTB's due to regulations of cross-border data flows.[28] The interdependence between, on the one hand, productivity growth and, on the other hand, exports, imports and investment is neglected in static CGE models.

#### *2. Treatment of Investment*

GTAP is a pure "real goods model" that does not account for financial instruments. Thus, the standard GTAP model does not take into consideration supply-side impacts of capital market conditions. In the model, investors are represented by a global bank allocating regional savings and investments around the world. Investment itself is represented by a stock of "capital goods" (CGDS), which is treated as a commodity that is purchased by the global bank and allocated to regions following a return-equalising rule. The capital goods commodity does not employ any primary factors of production. It rather absorbs a mix of intermediate goods such as construction, machinery equipment, vehicles, and services etc. In addition, capital goods cannot be traded across regions. Instead regional capital goods formation is determined be regional savings, which are absorbed by the global bank and reallocated to regions thereafter.[29] For a detailed description of the treatment of capital goods in GTAP see Malcom (1998).

In order to estimate the economic impact of decreasing returns on capital due to data localisation barriers to trade, we follow an indirect expected rate of return approach. It is assumed that the global bank allocates investment across regions in such a way that risk-adjusted rates of returns are equalised across regions. Thus, in GTAP a change of the expected rate of return in a given region results in corresponding changes in the amount of regional investment. The underlying assumption is that equilibrium rates of returns on investment are equal across regions and equal to a global rate of return. In addition, it is assumed that expected returns in a specific region will fall as the amount of investment rises. Thus, a difference between the global rate of return and a region's rate of return triggers a reallocation of investment across regions until regional rates of investment are equalised again. The difference between risk-adjusted regional rates of return can be read as a region-specific risk premium decreasing the region's attractiveness to investors. In line with this assumption, an increase in regional investment risk reduces capital goods formation and decreases demand for factor inputs to investment in the region concerned. At the same time, investment would increase in regions not affected by decreasing investor appetite.

The results of our experiment only have indicative character, meaning that we are not able to forecast the precise investment effect due to data localisation barriers to trade mainly for two reasons: 1) The shortcomings in the treatment of investment in GTAP and 2) the transformation of expected returns on investment into investors risk appetite, which is an empirical problem in general. Yet, the methodology we apply allows us to forecast and trace the direction of investment flows.

## BIBLIOGRAPHY

Andriamananjara, Dean, Feinberg, Ferrantino, Ludema, Tsigas (2004), The Effects of Non-Tariff Measures on Prices, Trade, and Welfare: CGE Implementation of Policy-Based Price Comparisons, USITC Economics Working Paper No. 2004-04-A.

Asia Sentinel, Indonesia May Force Web Giants to Build Local Data Centers, 27.01.2014, accessed at http://www.asiasentinel.com/econ-business/indonesia-web-giants-local-data-centers/, 12.04.2014.

Cassells, Meister, Cost and trade impacts of environmental regulations: effluent control and the New Zealand dairy sector. The Australian Journal of Agricultural and Resource Economics 45 (2), p. 257-274, 2001

A. Chander, U. P. Lê, Breaking the Web: Data Localization vs. the Global Internet, Working Paper 2014-1, California International Law Center, 12.03.2014, accessed at http://ssrn.com/abstract=2407858, 20.03.2014.

Christensen, L., A. Colciago, F. Etro and G. Rafert (2013) "The Impact of the Data Protection Regulation in the EU", Intertic Policy Paper, Intertic.

Covington & Burling LLP, China Releases New National Standard For Personal Information Collected Over Information Systems, E-alert Global Privacy & Data Security, 15.02.2013, accessed at http://www.cov.com/files/Publication/.../China_Releases _New_National_Standard_for_Personal_Information_Collected_Over_Information_Systems.pdf, 12.04.2014.

G. Cheah, Protection of personal financial information in China, Norton Rose Fulbright, October 2011, accessed at http://www.nortonrosefulbright.com/knowledge/publications/56148/protection-of-personal-financial-information-in-china, 12.04.2014.

China Copyright and Media, National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection, 28.12.2012, accessed at http://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/, 20.01.2014.

China Copyright and Media, Telecommunications and Internet Personal User Data Protection Regulations, 16.07.2013, accessed at: http://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/, 20.01.2014.

L. Clark, Tim Berners-Lee: we need to re-decentralise the web, Wired, 06.02.2014, accessed at http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web, 20.03.2014.

Cushman & Wakefield, Data Centre Risk Index 2013, accessed at: http://www.cushmanwakefield.pt/en-gb/research-and-insight/2013/data-centre-risk-index-2013

DLA Piper, Data Protection Laws of the World, accessed at http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf, 15.04.2014.

Elffers, Heijden, Hezewijk, Explaining Regulatory Non-compliance: A Survey Study of Rule Transgression for Two Dutch Instrumental Laws, Applying the Randomized Response Method, Journal of quantitative criminology, volume: 19 (2003), pp. 409 – 439, accessed

from [http://igitur-archive.library.uu.nl/fss/2007-0206-201216/64.%20Explaining%20regulatory%20non-compliance.pdf], 2003

Frost & Sullivan, Insights into Big Data and Analytics in Brazil, 2014

Koszerek, D., Havik, K., McMorrow, K., Röger, W., Schönborn, F. (2007), An Overview of the EU KLEMS Growth and Productivity Accounts

Foure, Benassy-Quere, Fontagne (2010), The world economy in 2050: a tentative picture, CEPII Working paper 2010-27.

Hertel, Tsiga, Structure of GTAP. In Global Trade Analysis : Modeling and Applications. Ed. Thomas W. Hertel, Purdue University. Cambridge University Press. 1997

Hunton & Williams LLP, Recent Data Breach Events in China, Privacy and Information Security Law Blog, 31.12.2013, accessed at https://www.huntonprivacyblog.com/2013/12/articles/recent-data-breach-events-china/, 20.01.2014.

Hunton & Williams LLP, Outsourcers Exempt from India's Privacy Regulations, Privacy and Information Security Law Blog, 24.08.2011, accessed at https://www.huntonprivacyblog.com/2011/08/articles/outsourcers-exempt-from-indias-privacy-regulations/, 18.03.2014.

Jorgenson, Ho, Stiroh, Information Technology and the American Growth Resurgence (Cambridge, MA: MIT Press), 2005

Library of Congress, Global Legal Monitor: Vietnam: Controversial Internet Decree in Effect, 06.09.2013, accessed at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403690_text, 13.12.2013.

Malcolm, G. (1998), Modeling Country Risk and Capital Flows in GTAP, GTAP Technical Paper No. 13.

V. Manuturi, B. Gokkon, Web Giants to Build Data Centers in Indonesia?, 15.01.2014, The Jakarta Globe, accessed at http://www.thejakartaglobe.com/news/web-giants-to-build-data-centers/, 02.03.2014

C. C. Miller, Google Pushes Back Against Data Localization, Bits Blog New York Times, 24.01.2014, accessed at http://bits.blogs.nytimes.com/2014/01/24/google-pushes-back-against-data-localization/, 27.03.2014.

Narayanan, G., Badri, Angel A. and McDougall, R., Eds., Global Trade, Assistance, and Production: The GTAP 8 Data Base, Center for Global Trade Analysis, Purdue University, 2012

Rakotoarisoa, M. A. (2011), A Contribution to the Analyses of the Effects of Foreign Agricultural Investment on the Food Sector and Trade in Sub-Saharan Africa.

M. Palmedo, Vietnam's Decree 72 on Internet Services Aims to Fight Piracy, Raises Human Rights Concerns, infojustice.org, 02.09.2013, accessed at http://infojustice.org/archives/30620, 27.03.2014.

PTI, RIM finally sets up Blackberry server in Mumbai, 20.02.2012, accessed at http://timesofindia.indiatimes.com/tech/tech-news/RIM-finally-sets-up-BlackBerry-server-in-Mumbai/articleshow/11963492.cms, 20.03.2014.

Thanguvalu, S. M. and Rajguru, G. (2004), Is There an Export or Import- Led Productivity Growth in Rapidly Developing Countries? A Multivariate VAR Analysis, Applied Economics, Vol. 36, pp. 1083-1093.

UK Ministry of Justice (2012) "Impact Assessment for the Proposal for an EU Data Protection Regulation", London: UK Government.

US Bureau of Economic Analysis, Input and Output Accounts Data, 2007

Xu, Zhu, Gibbs, Global technology, local adoption: A cross-country investigation of Internet adoption by companies in the United States and China, Electronic Markets, 2004

## ENDNOTES

1. European Commission, Staff Working Paper, SEC (2012) 72 final

2. OECD (2013), Product Market Regulation Database, www.oecd.org/economy/pmr

3. Data on TFP and prices for each sector are taken from EUKLEMS, whereas intensities of data services for each sector are based on US input/output use tables from the US Bureau of Economic Analysis (BEA).

4. Christensen, L., A. Colciago, F. Etro and G. Rafert , The Impact of the Data Protection Regulation in the EU, Intertic Policy Paper, Intertic, 2013; UK Ministry of Justice, Impact Assessment for the Proposal for an EU Data Protection Regulation, UK Government, 2012

5. Cushman & Wakefield, Data Centre Risk Index 2013, accessed at: http://www.cushmanwakefield.pt/en-gb/research-and-insight/2013/data-centre-risk-index-2013

6. Frost & Sullivan, Insights into Big Data and Analytics in Brazil, 2014

7. Xu, Zhu, Gibbs, Global technology, local adoption: A cross-country investigation of Internet adoption by companies in the United States and China, Electronic Markets, 2004

8. Computer Economics, 2011

9. L. Clark, Tim Berners-Lee: we need to re-decentralise the web, Wired, 06.02.2014, accessed at http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web, 20.03.2014.

10. A. Chander, U. P. Lê, Breaking the Web: Data Localization vs. the Global Internet, Working Paper 2014-1, California International Law Center, 12.03.2014, accessed at http://ssrn.com/abstract=2407858, 20.03.2014.

11. Netmundial draft conclusions, section I, art 4

12. Hunton & Williams LLP, Recent Data Breach Events in China, Privacy and Information Security Law Blog, 31.12.2013, accessed at https://www.huntonprivacyblog.com/2013/12/articles/recent-data-breach-events-china/, 20.01.2014.

13. China Copyright and Media, National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection, 28.12.2012, accessed at http://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/, 20.01.2014.

14. Covington & Burling LLP, China Releases New National Standard For Personal Information Collected Over Information Systems, E-alert Global Privacy & Data Security, 15.02.2013, accessed at http://www.cov.com/files/Publication/.../China_Releases _New_National_Standard_for_Personal_Information_Collected_Over_Information_Systems.pdf, 12.04.2014.

15. G. Cheah, Protection of personal financial information in China, Norton Rose Fulbright, October 2011, accessed at http://www.nortonrosefulbright.com/knowledge/publications/56148/protection-of-personal-financial-information-in-china, 12.04.2014.

16. China Copyright and Media, Telecommunications and Internet Personal User Data Protection Regulations, 16.07.2013, accessed at: http://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/, 20.01.2014.

17. A. Chander, U. P. Lê, Breaking the Web: Data Localization vs. the Global Internet, Working Paper 2014-1, California International Law Center, 12.03.2014, accessed at http://ssrn.com/abstract=2407858, 20.03.2014.

18. Sensitive personal data includes physical, physiological and mental health conditions, medical records and history, and sexual orientation. The definition also includes biometric data, passwords and financial information such as bank account details, credit and debit card details.

19. Hunton & Williams LLP, Outsourcers Exempt from India's Privacy Regulations, Privacy and Information Security Law Blog, 24.08.2011, accessed at https://www.huntonprivacyblog.com/2011/08/articles/outsourcers-exempt-from-indias-privacy-regulations/, 18.03.2014.

20. PTI, RIM finally sets up Blackberry server in Mumbai, 20.02.2012, accessed at http://timesofindia.indiatimes.com/tech/tech-news/RIM-finally-sets-up-BlackBerry-server-in-Mumbai/articleshow/11963492.cms, 20.03.2014.

21. DLA Piper, Data Protection Laws of the World, accessed at http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf, 15.04.2014.

22. Asia Sentinel, Indonesia May Force Web Giants to Build Local Data Centers, 27.01.2014, accessed at http://www.asiasentinel.com/econ-business/indonesia-web-giants-local-data-centers/, 12.04.2014.

23. DLA Piper, Data Protection Laws of the World, accessed at http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf, 15.04.2014.

24. Library of Congress, Global Legal Monitor: Vietnam: Controversial Internet Decree in Effect, 06.09.2013, accessed at http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403690_text, 13.12.2013.

25. M. Palmedo, Vietnam's Decree 72 on Internet Services Aims to Fight Piracy, Raises Human Rights Concerns, infojustice.org, 02.09.2013, accessed at http://infojustice.org/archives/30620, 27.03.2014.

26. Hertel, Tsiga, Structure of GTAP. In Global Trade Analysis : Modeling and Applications. Ed. Thomas W. Hertel, Purdue University. Cambridge University Press. 1997

27. For further information on original data and model components see Hertel and Tsigas (1997).

28. The static GTAP 8 model does not account for the effects of trade liberalization on domestic industries' productivity growth. Trade liberalization, however, may cause productivity to rise. See, e.g., Thanguvalu and Gulasekaran 2004 who study export and import led productivity growth in developing countries. The authors find empirical evidence that increasing imports have a positive effect on long-term output growth.

29. See Malcolm (1998) and Rakotoarisoa (2011).