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

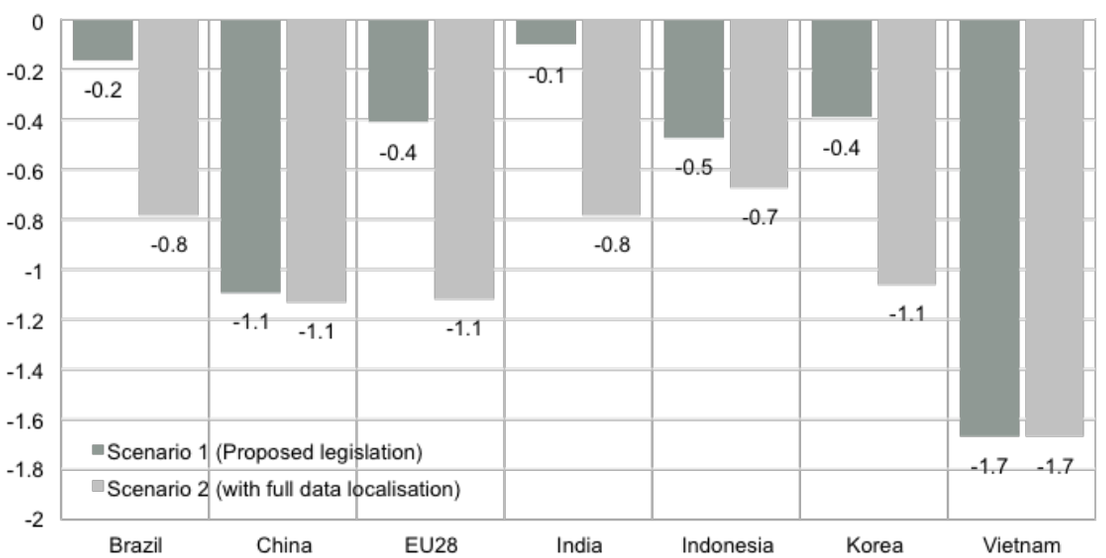
market limitations, investments made by both domestic and foreign entities will decrease. In GTAP8 this is introduced as a change in rate of return on investments (see Annex II). Furthermore, a final shock occurs as an additional effect on the return on investment, which is derived from research and 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 %

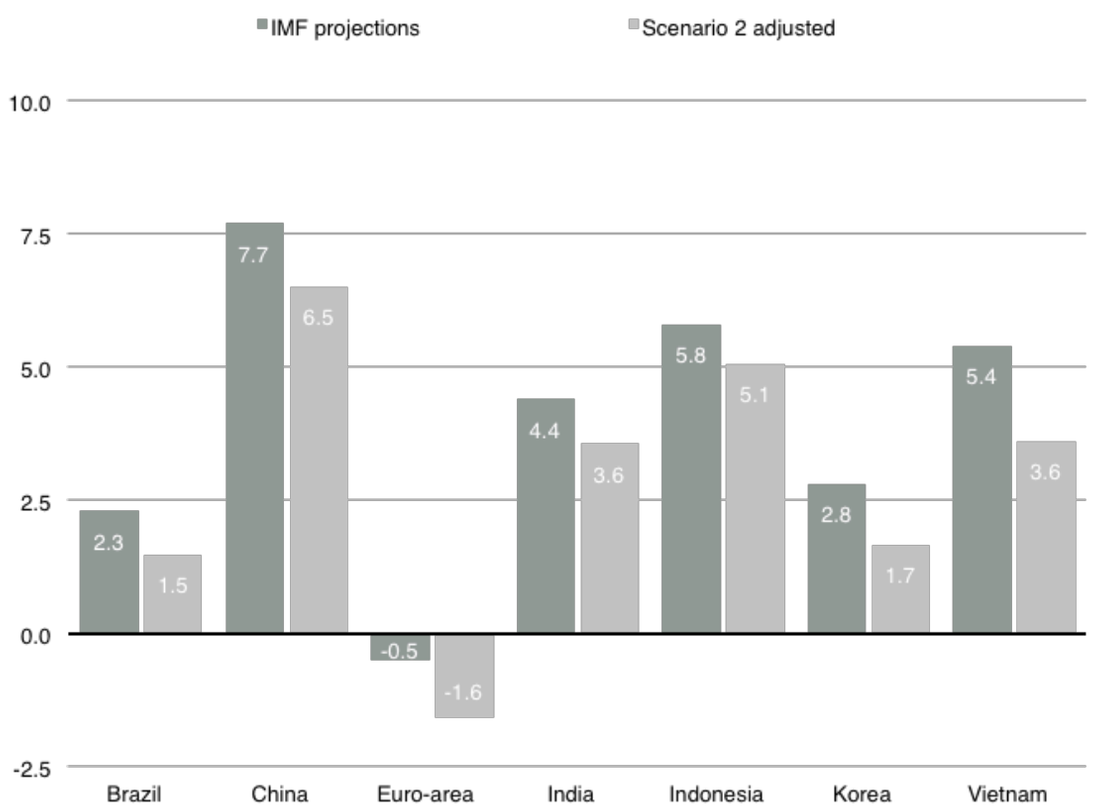
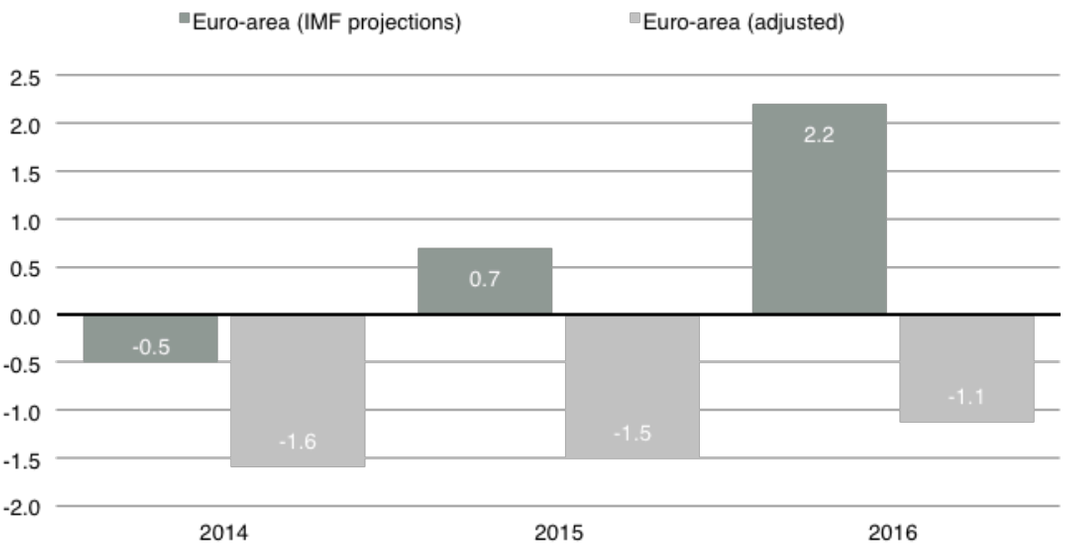


FIGURE 3: PROJECTED GDP GROWTH FOR THE EURO ZONE ACCUMULATED CHANGES IN % SINCE 2013



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 %

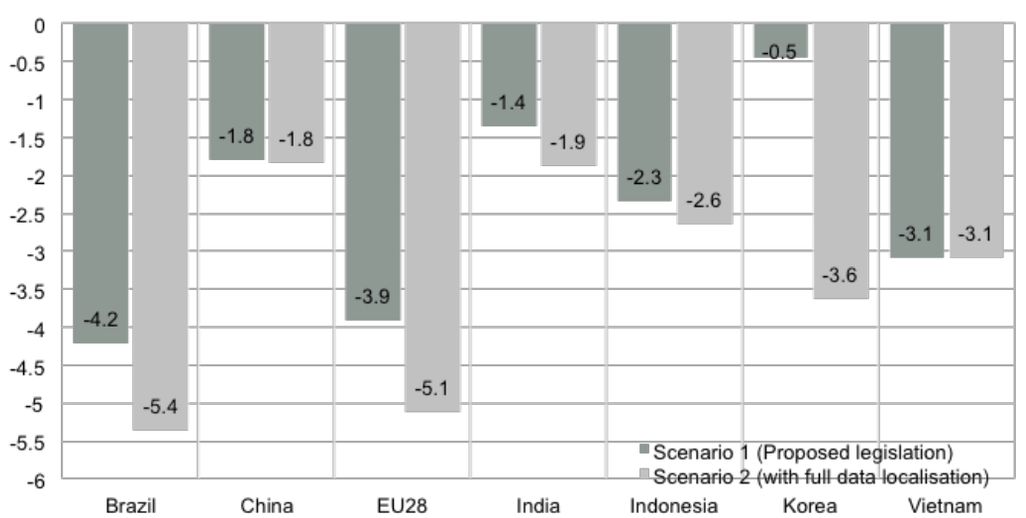
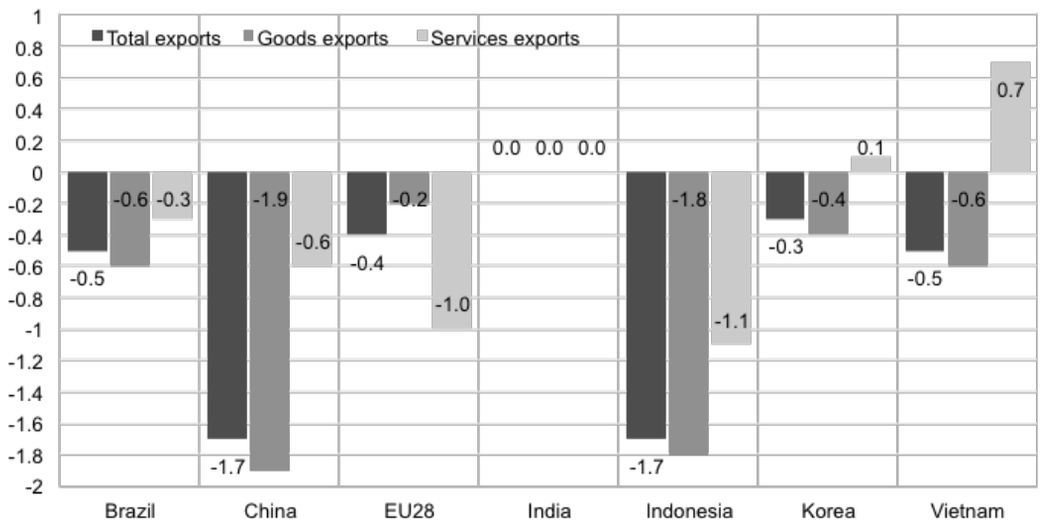


Figure 5 finally sets out the changes for trade, both in terms of total exports, goods exports and services exports. First we note that the exports effects are lower than the investment changes reported in Figure 2. A second interesting issue with regards to the trade effects is that for some countries 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).