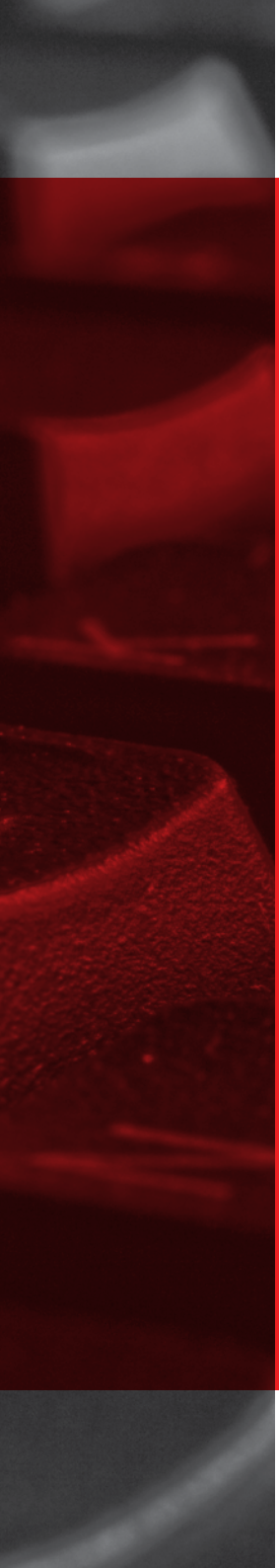
Data localization laws in a digital world

Data protection or data protectionism?

Neha Mishra
LLM in Public International Law, Class of 2011, London School of Economics and Political Science
Master in Public Policy, Class of 2015 National University of Singapore



ABSTRACT

Data localization laws are emerging as a pernicious form of non-tariff barrier which significantly harms the growth of trade in a digitally powered world. An International Political Economy approach provides a more comprehensive analysis of the policy rationale behind such laws, as compared to a purely economic approach, which only focuses on economic losses resulting from protectionism. On a closer analysis, it is found that different countries may have different policy rationales for implementing data localization laws – while some promote their domestic ICT industry through forced localization measures, others have concerns regarding national security, privacy, and ensuring sovereign control in the highly privatized world of internet governance. It is not always possible to demarcate the "protectionist" rationale from that of rational "data protection". To address data localization effectively and facilitate digital trade, it is not sufficient to negotiate for free flow of data in trade agreements without Governments and companies being open and transparent about the related issues of privacy, national security and consumer protection. Particularly, the role of US Government as well as leading US-based technology companies will be instrumental in this regard. At the same time, it may be necessary to develop policy initiatives both to encourage transparent and clear international standards on data security, as well as to enable higher levels of digital innovation in developing countries such that they can harness the benefits of evolving internet technologies.

INTRODUCTION

The new wave of policies preventing free flow of data across borders is feared to be one of the most critical barriers to 21st century trade. Several experts both within the industry and outside consider such restrictions to be unsustainable policy practice as the free flow of data through the internet powers a majority of transactions in the world today (Ezell *et al*, 2013; McKinsey Global Institute, 2014; Donnan 2014; Chander and Le, 2014). Furthermore, critics are sceptical as to whether data localization initiatives generate any value addition to the domestic economy at all (Baeur *et al*, 2013; 2014; 2015). Nonetheless, several Governments continue to adopt a range of data localization laws for a variety of policy objectives, from safeguarding the data privacy of individual citizens and guarding their (data) sovereignty to promoting the growth of a domestic digital economy (Chander and Le, 2014; Castro and Mcquinn, 2015, US Chamber of Commerce and Hunton & Williams, 2014). It is particularly striking that data localization policies are proliferating across both liberal/democratic states such as Australia, Canada, and India, as well as illiberal regimes such as China, Vietnam and Iran. The latest to join was Russia, which implemented its data localization law in September 2015, with the stated policy objectives of national security and the protection of privacy of Russian citizens (Bowman, 2015; Kurochkin *et al*, 2015). Sceptics suspect that these policies are more likely to be instrumental in repressing any political dissent through online platforms and preventing the free flow of information from the outside world to Russia. The impact of Russia's laws is further expected to have an adverse affect on businesses and cross-border trade, with estimated economic losses amounting to 0.27 per cent of GDP – particularly harmful in a time of severe economic recession (Lee-Makiyama, 10 June 2015).

The purpose of this paper is to study data localization laws from an international political economy (IPE) perspective, its re-

percussions, and its policy implications for rules governing digital trade. This exercise is vital to understanding the environment in which data localization laws take force. It is also an important starting point to assess the extent to which trade policy is suited to address regulatory challenges of the digital world today. The majority of existing scholarship on this issue tends to focus on the liberalization of digital trade and the necessity of the cross-border flow of data, which, while compelling, is insufficient to unravel the complex regulatory dilemmas associated with digital data management. While some believe that forced data localization is a deliberate strategy to protect the domestic economy and undercut competition from American IT giants (Lee-Makiyama, 2013; Chander and Le, 2014; Aaronson and Maxim, 2013), others are more sympathetic towards concerns regarding data privacy, surveillance, and guarding the data sovereignty of countries (Rubin, 2015; Kong, 2010). This paper emphasizes that the policy rationale for implementing data localization laws in a country may often be contextual and an outcome of the interaction between "markets" and "politics" in which a given government operates (Gilpin, 2001).

The first part of the paper provides an overview of data localization laws across the world, their desired policy objectives, and their impact on the innovation economy at large. The second part of the essay is a critical evaluation of the IPE of data localization policies. A clear distinction is drawn between the economics and the IPE of data localization policies to evaluate the larger policy environment in which laws for digital trade operate. The third part provides recommendations to engage with the issue of data localization more effectively and meaningfully, taking into account both the economic and political realities. The paper concludes by suggesting that trade rules are one of the constituent elements of the larger digital trade economy and may have limited impact in addressing data localization problems unless countries are willing to negotiate on interconnected issues of privacy, con-

sumer protection and data sovereignty. The latter necessitates enhanced standards of transparency, international cooperation and political compromise at a global level.

DATA LOCALIZATION LAWS AND THEIR IMPACT ON TRADE

Implementation of data localization laws became vigorous in the aftermath of the Snowden affair in June 2013, which brought damning evidence to the international community of the extent to which the US National Security Agency had been surveilling online information of both American and foreign citizens and companies (Dhont and Woodcock, 2015; Donnan, 14 August 2014; Donohue, 2015; Hill, 2014). However, the move towards data localization predates the Snowden incident. For instance, as early as 2005, the Government of Kazakhstan passed a law requiring that all data sited in the .kz domain be located domestically, but later made an exception for technology companies such as Google (Castro and Mcquinn, 2015). Requirements for data localizations or restrictions on free flow of data have been made in recent years in countries such as Vietnam, Indonesia, Brunei, Iran, China, Brazil, India, Australia, Korea, Nigeria and, most recently, Russia (For details, see Chander and Le, 2014; Castro and Mcquinn, 2015, Dhont and Woodcock, 2015; Svatesson, 2010). It should be noted that while some of these countries impose a blanket ban on the transfer of all categories of personal data abroad, others, such as Australia and South Korea, impose specific restrictions on the transfer of data in sectors such as health and finance on grounds of protecting citizens' sensitive data. For some countries, such as Malaysia and the Philippines, strict consent requirements and regulatory approvals for overseas data transfer exist, which tend to slow down the process and often result in forced data localization. Some countries such as India

also require foreign companies to enter into local partnerships to provide various IT services (Hill, 2014). In many of these countries, it appears that data localization requirements are pushed as a protectionist measure to boost the domestic digital economy while – especially in the case of Russia, China, Vietnam and Iran – there are added concerns of state control and censorship of data (Atkinson, 2010; Hill 2014; Chander and Le, 2014; Bajoria, 5 June 2014).

The EU is considered to be one of the strictest regimes in the world for data privacy. EU regulations prohibit the transfer of data belonging to EU residents to outside jurisdictions lacking "adequate" data privacy regimes. However, companies who meet the required standards under the regulation are deemed to qualify for "safe harbour" protections (Directive 95/46/EC, 24 October 1995). In 2012, the European Commission proposed a unified regime called the General Data Protection Regime ("GDPR") which imposes much stricter standards on data privacy and protection in light of new technologies such as cloud computing and the rise in social networking. A study commissioned by the American Chamber of Commerce (Bauer *et al*, 2013) estimated that the implementation of GDPR would reduce the GDP of the EU between 0.8 to 1.3 percentage points. Furthermore, if the 'right to be forgotten' rule was incorporated in the GDPR, the losses to GDP would be far higher, in the range of 1.5 to 3.9 percentage points (See also Ezell *et al*, 2014). While some argue that the EU data privacy regime is grounded in the cultural context (Milberg *et al*, 2000), others highlight that the proposed regime is disproportionate and excessive, and potentially protectionist (Lee-Makiyama, 2013; Baeur *et al,* 2013). The EU maintains that their privacy regulations make a legitimate distinction between rational protection of data and data protectionism (Panel discussion on Trade Agreements and Data Flow [see statement of Ignatio Irrurarezaga, Head of Unit on Services, DG Trade], 30 July 2015). It is not easy to assess this distinction in practice.

For instance, in recent years, several technology giants such as Microsoft, Google, Apple and Amazon have built data centres in Dublin and Denmark (The Irish Times, 5 March 2015; Apple Press Info, 23 February 2015). It is perhaps also noteworthy to mention that, from the Snowden revelations to the dispute between Max Schrems and Facebook (Judgment in Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner, "Schrems case"*), it has been contended that several American companies which enjoy safe harbour protection do not have privacy protection tantamount to the EU legal standard (Crawford, 26 March 2015). The recent CJEU judgment in the *Schrems* case invalidated the US-EU Safe Harbour Argument and thereby raises problematic questions on current business models of digital trade, even though press reports had previously indicated the possibility of a political compromise on the EU-US Safe Harbour Agreement (Reuters, 2015). As expected, in several recent trade negotiations such as the Transatlantic Trade and Investment Partnership (TTIP), the EU is under pressure to advocate for higher standards of data privacy in order to win greater public trust within their domestic jurisdiction(s), while there is strong pushback from the US.

One of the basic problems with complying with data localization laws for companies is the difficulty in determining which categories of data need to be locally stored and which can be moved abroad. A recent study indicates that distinguishing personal data from non-personal data for purposes of data localization is a complex issue (Bauer *et al*, 2015). Legal experts also have a problem in assessing the legal liability of foreign companies who do not have a business presence in a country but may be handling large quantities of data of citizens in the course of normal day-to-day business transactions in the global marketplace. Furthermore, when companies are forced to relocate their servers to jurisdictions with low levels of internet security, concerns arise regarding possible breaches of consumer trust,

which may invite further legal liability. Finally, foreign companies are also worried to operate data centres in several authoritarian jurisdictions where state censorship and surveillance laws are over-encompassing and create significant liabilities for service providers. While these laws fail to satisfy their objective of providing adequate security and privacy to user data, they create several economic and technical drawbacks which can prejudice the resilience and the utility of the internet as a platform for communication and trade. Discussed below are the main drawbacks of data localization, which not only prejudice economic benefits from digital trade, but also hamper data security and interfere with the broader architecture of the internet.

First, several studies have shown that the free flow of data is not only critical for information and communication technologies (ICT) services, but of paramount importance to trade in goods and services in general (For an elaborate discussion, see Van-der Marel, 2015). This not only affects the global economy, but also countries that implement such measures, thus counteracting any potential policies to boost the local market (Ezell *et al*, 2013; McKinsey Global Institute, 2014; Donnan, 2014; Baeur *et al*, 2013; 2014; 2015). For instance, a study by McKinsey (2014) showed that 75 per cent of the value addition from data flows goes to traditional manufacturing industries while another study by United Nations Conference on Trade and Development (UNCTAD) showed that 50 per cent of all traded services are enabled through the ICT industry (Castro and Mcquinn, 2015). A recent study by ECIPE (Bauer *et al*, 2014) has shown that restriction on cross-border data flows adversely impacts countries which adopt such laws – for instance, in Indonesia, data localization laws could reduce GDP by 0.7 per cent and reduce investments by 2.3 per cent. Similar results were also recorded for South Korea and the EU (Baeur *et al*, 2013; 2014; 2015). As cross-border trade increasingly moves towards e-commerce and relies on the use of internet technologies such as cloud computing

and big data, data localization policies pose a major threat to the economy. Not surprisingly, several business associations (mostly consisting of global market leaders based in the US) (AmCham China, 2015; Information Technology Industry Council, 15 October 2014; Asia Internet Coalition, 2014; US Chamber of Commerce, 2015) as well as a few governments (most evidently, the US government) (Office of the United States Trade Representative [USTR], 2015), have presented a strong economic case for the free flow of data in various regional trade agreements such as the Trans Pacific Partnership (TPP), Trade in Services Agreement (TISA) and TTIP.

Second, data localization laws do not necessarily provide a solution to problems of data breaches or boosting data security. On the contrary, by compelling forced localization of data, these laws are very likely to make data more vulnerable to both security attacks and natural disasters, as the data no longer undergoes sharding[1](Heidt, 2015). Particularly, in countries with poor IT security systems, data localization defeats the purpose of data protection. Further, several foreign governments such as the US use sophisticated malware for data surveillance – hence, simply relocating data is of no use. Moreover, there is an increased risk of local surveillance through implementation of such laws (Chander and Le, 2014; 2015).

1. In the process of sharding, data is partitioned and stored over multiple physical locations, rather than one location.

Third, mandating localization of data centres is against the economic logic of the technology industry, which is primarily based on global economies of scale. Furthermore, localization raises costs, and reduces competitiveness and productivity for both local consumers and businesses (Ezell and Atkinson, 2010). It is also detrimental to several modern-day innovations in big data, cloud computing and "Internet of Things", which bring several benefits to any local economy, including higher levels of efficiency and cost-effectiveness in businesses. More importantly, data centres are largely automated – hence, they do not generate significant levels of employment, though upfront investment and

long-term energy costs are very high (The Wall Street Journal, 13 November 2013; ZD Net, 2 April 2013).

Finally, data localization initiatives adversely impact the overall structure of the current form of internet governance, which is based on a world-wide network of exchange of information and data. Localized data centres may result in splintering the internet ("splinternet"), which is unlikely to be rewarding to businesses and consumers alike (US Chamber of Commerce and Hunton & Williams, 2014). Moreover, if country A does not trust country B to host its citizens' data, the reverse is also likely to be true, ultimately leading to disruption of an interconnected network.

From the discussion above, it is evident that the costs of data localization are too high and the achievement of desired policy outcomes mostly uncertain. Particularly, Governments have the option of adopting alternate standards such as enforcing strict end-to-end encryption standards based on a recognized international standard instead of imposing measures that restrict trade and innovation. However, governments increasingly adopt localization measures, both in the developing and developed world alike. This begs the fundamental question regarding policy motivations that result in implementation of data localization laws.

DATA LOCALIZATION FROM AN IPE POINT OF VIEW

From an IPE perspective, a dominant view is the emergence of "innovation mercantilism" in digital trade today (Ezell *et al,* 2013; Atkinson, 2010). Prior to the widespread adoption of liberal values, mercantilism (or economic nationalism) prevailed from the 16th to 18th centuries. The prevailing policies in mercantilism include a favourable balance of trade, protection of domestic industries, boosting local employment, species accumulation, and manipula-

tion of exchange rates to keep exports competitive (*The Economist,* 23 August 2013; Douglas, 1991; Rodrik, 2013). However, scholars repeatedly indicate that certain aspects of mercantilist practice play an important role in doctrines of classical liberalism (Grampp, 1952). For instance, classical liberalists like Adam Smith argued that national security was an important exception to free trade. He also acknowledged that states cannot merely be driven by an economic logic of the market, but will also be driven by social interests such as protecting the people who emerge as losers in a free market (Walter, 1996). Even liberal governments regulate economic activity and provide protection or financial support to some groups within their country based on their political power or, more rarely, on grounds of social justice.

With this background in mind, it is important to explore how the political economy has evolved as digital data has become the "new currency" in international trade. There is a perception that in a digital world, countries that have access to more data are in a better position to maximize their wealth and power. It is therefore not surprising that more and more developing countries make an effort to prevent the export of data across borders or even tax the flow of data, with the hope that it would drive greater innovation, generate more revenues for local enterprises, and drive investment into the domestic economy. To trade practitioners, this is a familiar case of infant industry protection through non-tariff measures. Further, countries (particularly those with larger populations and/or resources, such as China) are likely to consider data localization as a strategic tool to gain control over more data at home and abroad, thereby providing credible competition to some of the biggest American players who dominate the market today. Again, many trade practitioners would recognize this is as a use of a non-tariff barrier to gain greater market shares. However, this narrative is incomplete in terms of recognizing several other strategic interests (aside from gaining trade) that drive domestic policies in the digital world today.

Services such as cloud computing, e-commerce, and big data processing now allow some of the biggest American internet companies to collect and control vast amounts of data. Many developed countries and fast-developing economies such as China recognize that overpowering American leadership in digital space is only possible if they develop indigenous data processing facilities that reach a larger chunk of the global market. The trade war between the US and China is particularly instrumental in understanding the policy context. Other developed countries such as Germany, France, Norway and Australia also aspire to become key leaders in the digital economy (Chander and Le, 2015). However, the power competition is not merely for economic gains, but equally for political ones. As both American and Chinese companies have access to greater amounts of data, their political power and control increases significantly and extends well beyond the realms of trade. This was evident when the US blocked the use of Huawei products on the suspicion that it would provide backdoor access to data located within the US to the Chinese government (BBC News, 2014). Similarly, China has successfully blocked the likes of Google and Facebook from operating within their jurisdiction – arguably not only with the intention of generating more business opportunities for local players, but also based on strategic political interests. The developments in the EU are also equally interesting. With the increased suspicion of American surveillance, the EU, which enjoys a reputation for strict enforcement of data protection, now has new players from France, Germany and Norway who claim that their digital services are surveillance-free, aiming to appeal to both the EU and the global market (Chander and Le, 2015).

At the same time, a large number of developing countries, including Brazil, India, Indonesia and several other fast developing countries in Southeast Asia, are aiming to expand their reach in global markets through data localization policies. Even some relatively less developed countries, such as Nigeria, are eager to

expand their digital economy and are therefore keen on building local data centres. Often, their policy impetus for data localization laws is stated to be privacy and national security, although it is arguably a policy tool to conceal protectionism. It is often assumed that local data centres will create greater employment, skills upgrading and an overall improvement in the economy; in other words, help developing countries to move up the global value chains. This narrative can be very politically appealing, particularly given that it evokes a sense of nationalism and self-sufficiency. Consider the example of Indonesia: the strong wave of economic nationalism in various spheres of economic activity resulted in massive support for the government, but has so far resulted in limited returns to the economy (The Economist, 7 May 2015; The Economist, 7 May 2015a). It particularly results in causing harm to smaller, local businesses, who are deprived of cost-effective, secure services provided by several foreign players, which consequently tends to increase their transaction costs significantly (ITI, JEITA and Digital Europe, 2014; eBay, 2015).

In countries with monopoly telecom providers (usually state-owned), there is a high incentive for telecom lobby groups to block out foreign competition. Business estimates increasingly show that many of these companies are entering the cloud computing markets and ousting their foreign counterparts (Kehl et al, 2014). For instance, in Russia, the two most important gainers from the data localization law would be Rostec, a state-owned entity, as well as Rostelcom, the monopoly telecommunications provider in Russia (Data Centre Knowledge, 2015). Several of these developing countries, however, do not have appropriate infrastructure in place to set up secure and efficient data centres. This includes a secure technical infrastructure as well as an appropriate legal regime. For instance, internet fraud rates are highest in the world in Brazil, while in the past years Indonesia has shared a similar reputation for cybercrime (NPR, 2015). Even the Data Centre Risk Index, which ranks coun-

tries in terms of technical, economic and political security of data centres, finds that several jurisdictions implementing data localization laws such as China, Brazil, Indonesia and Russia are ranked very low (Cushman and Wakefield, 2013). Further, supporting laws such as privacy laws, data protection laws, IP laws, as well as laws to protect against political persecution, are essential to maintain integrity and stability of data centres; this is often missing in many developing countries (UNCTAD, 2013; Cushman and Wakefield, 2013).

There is no systematic study to date that shows that there are any foreseeable positive returns to the economy through data localization, either from the additional investments or the technology transfer that comes in when a foreign company relocates its servers to a country. In fact, companies have strong economic (and often strategic) reasons for locating their servers in other parts of the world – hence, forced localization of data centres may not reap the expected economic returns. However, states are not just interested in increasing revenues for their own economy, but also in their position relative to other countries, commonly known as relative gains. States are often driven by relative gains, even at the cost of sacrificing absolute gains (Krasner, 1976). For instance, the Indonesian or Vietnamese government would be more keen to have the likes of Google and Microsoft open up data centres in their country rather than in neighbouring Thailand or Malaysia, even though it is very likely that their domestic markets are less equipped to host data centres and would benefit more by using foreign data centres. Although economically counter-intuitive, the idea of relative gains is an important driver of national policy as it finds surprising levels of political support (Drezner, 2012).

The other important idea driving state policy is the protection of national autonomy. First, it is important to remember that the internet governance mechanism in the past has been heavily privately managed (by bodies such as ICANN) and has

often been predominantly US-centric. The idea of sovereign control over flow of information over the internet was not given much policy attention for several years. However, this resulted in a "complex cyber regime complex" with a multitude of actors (often private) and institutions. As Nye (2014) effectively puts it, this was a compromise between "a single coherent legal structure and complete fragmentation of normative structures" in cyberspace. Progressively, it is becoming clearer that a sovereignty-based model is irrelevant in a digitally connected world. Rather, a multi-stakeholder approach with a variety of institutional and private actors, and a variety of interests going well beyond trade (human rights, internet governance, surveillance and privacy), may be necessary. This increasingly appears as a threat to the domestic sovereignty that countries enjoy in trade negotiations in bodies such as the WTO.

Moreover, US-based companies currently enjoy an almost hegemonic status in the digital world. As a result, there is significant apprehension that the US government exercises strong control over the data goldmines, and reap disproportionate economic and political benefits. These views have been particularly strengthened post-Snowden. Many governments are able to generate political buy-in for adopting stringent consent regimes for data transfer and high thresholds of data protection, as it is likely to weaken American hegemony channelled through technology giants based out of the US. Furthermore, the privately-regulated nature of the internet, along with non-transparent actions of the US Government, are likely to make countries wary of letting data on its citizens flow freely out of the country. In fact, trade forums such as the WTO barely touch upon privacy and transparency issues within the internet. Therefore, despite the strong economic logic for letting data move around freely, it appears legitimate for countries to be concerned about national security and the preservation of autonomy. These exceptions are also well built in the WTO Agreements such as under Article XIV and XIV: bis of GATS.

One of the most effective ways of allowing for safe transmission of data online is to execute end-to-end encryption of data. This raises interesting questions of sovereignty and standard-setting. While technology companies should ideally develop trustworthy and secure standards to encrypt data, bodies such as the Federal Bureau of Investigation in the US have required companies to have a backdoor mechanism by which they could break the encryption in case of sensitive investigations (The Guardian, 8 July 2015). This raises important questions of transparency and trust in the standards that are used in digital services and goods. Particularly, since standard regulation of the internet tends to be based on private protocols and often set by American companies, other sovereign states are likely to consider it an affront to their sovereignty because they have no say in the adoption of such standards. Further, once data resides abroad, they do not exercise any jurisdictional control over such data. Therefore, countries may also develop indigenous standards for data encryption in order to avoid extra-territorial surveillance. For instance, Chinese digital products and services provide for end-to-end encryption, which is developed locally. For the American Government, this is not only viewed as a cause of suspicion, but also an affront to the position of domination of American companies in technology trade. The issue of law enforcement in the digital world also creates an incentive for data localization. Particularly, with the increase in the rates and scale of cybercrimes, governments cannot afford to ignore issues of law enforcement. Mulvenon and Denmark (2010) argued that the global cyber commons is comparable to the Wild West of the 1870s and 1880s, where rule of law barely prevailed and it was up to each individual to take care of themselves. Similarly, in the absence of any cohesive rules in the current digital space, internet users are more or less responsible for ensuring their security.

Evidently, there is a discord between the economic logic behind allowing cross-border data flows – discussed in the previ-

ous section – and the political economy of data localization policies. In fact, the discussion dictates that existing dialogue on data localization touches upon clashing political philosophies and is not solely a case of straightforward data protectionism. The existing discourse on data localization makes compelling economic and technical arguments as to why data localization policies are harmful for trade, investment, cyber security and innovation. However, it fails to understand the strong political rationale driving such policies and the complex political economy of the digital world.

STRIKING THE RIGHT BALANCE

The contentious issues with respect to data localization extend well beyond free trade versus protectionism into some delicate, complex and legitimate political concerns, such as technology transfer and IP rights, privacy, human rights, and national security, which is currently missing (and expectedly so) on most trade agendas. To take an example: in the course of the TTIP negotiations, it became clear that addressing issues of data protection and privacy along with the free flow of data was inevitable to reach any kind of consensus between two great powers; the US and the EU (Kong, 2010). Similar possibilities exist with respect to the TPP, even though the US holds a dominant negotiating position. In fact, time and again, the US Government's reluctance to engage on issues of privacy and transparency, combined with its agenda on unhindered liberalization of data flows, has caused severe discontent amongst both developing and developed countries in negotiations of various Regional Trade Agreements (RTAs). Some scholars and business associations (often US-centric) have suggested taking stronger actions in trade forums such as the WTO or using the instrumentalities of USTR and mega-regionals such as the TPP to prevent restrictions on

cross-border data flow. For instance, the Trade Bill introduced in the Senate in 2013 (S. 1788, 113th Congress, 2013-14), *inter alia*, proposed negotiating for free flow of data and prevention of data protectionism in US trade negotiations. These measures are often viewed as a US strategy to maintain its position in the digital market and wipe out potential competitors.

Notably, the WTO is also ill-equipped (with its current arrangements) to become a focal centre for negotiations on cross-border data flows or addressing disputes related to these matters. Issues related to data protection and privacy often involve a plurality of interests and competing points of view (often embedded in deeper political philosophy of the countries and other relevant actors (See Post, 2001)); a consensus-based forum such as WTO barely facilitates any possibility of a compromise. Countries such as India and Brazil feel unprepared to negotiate on issues related to e-commerce (Livemint, 30 July 2015), which is likely to include discussions around free flow of data. Chander (2009) recommends the adoption of a "glocalization" approach in digital space, where laws can be harmonized globally, paying specific attention to local interests. This paints an optimistic scenario of extreme international cooperation on issues of internet standards and interoperability, mutual respect for domestic cultures and legal cooperation through treaties such as the Mutual Legal Assistance Treaties to enable free flow of data. A realist may dismiss this as a utopian state of affairs.

A more pragmatic approach to address concerns regarding data localization could be to incentivize governments across the world (particularly the developing world) to allow data to flow across borders freely. This could be done by creating opportunities for local businesses to harness the multiplier effect of innovations in big data and cloud technology (say for instance, the potential opportunity for digitally powered local companies and SMEs to participate in worldwide e-commerce markets [eBay, 2015]), while removing misunderstandings surrounding secu-

rity of cloud and big data technologies. Rather than using pressure tactics in trade forums such as RTA negotiations, the US government could show more engagement with issues related to sensitive political concerns. Countries such as the US, Australia and Singapore, which host global data centres, are likely to be viewed with suspicion, particularly when American companies are involved. There is a need to push for greater commitment and transparency from the US Government and American IT giants, in particular, to engage in a public dialogue to gain trust from their foreign counterparts. This can be coupled with a greater effort by technology companies to emphasize that the setting up of data centres alone has limited economic returns but investments in technology innovations (whether foreign or local) generates manifold increase in economic returns to traditional manufacturing sectors.

It is also important to highlight to governments the potential dangers of having insecure domestic systems, particularly if they store sensitive data. Ensuring data security is not simply based on the geographical location of the data servers, but also critically depends on the security and robustness of IT systems. More often than not, larger companies are better situated to ensure these services than local companies. In particular, this is likely to raise issues of standard-setting. Through transparent processes and open deliberations, international organization such as the ITU can enable such discussions amongst countries.

CONCLUSION

It is much a more comprehensive and viable policy approach to view trade negotiations for the free flow of data as a political economy issue rather than a strictly economic one. Although data localization laws have the capacity to fracture the digital trade ecosystem, political priorities cloud the policy space with

illusive promises of economic growth and data sovereignty, which need to be addressed head-on. Economic efficiency is not the sole benchmark in policy choices – concerns related to trust in digital goods and services cannot be ruled out. Powerful internet companies, along with their host governments, will need to be more transparent and ethical regarding the use of personal data. This will also increase the possibility of engaging in more policy innovations in the digital space, which is likely to undercut the wave of data localization. A good example in this regard is the adoption of data categorization standards in cloud computing, which allows for automatic cross-border transfer of most routine transaction data, and only imposes additional legal and security requirements for politically sensitive or highly secure data. In particular, as most of these policy innovations tend to start in the private realm, transparency is critical. Recognition and reconciliation of the multitude of interests and ideologies in digital trade is not easy – however, ignoring these complexities in trade agreements will most likely be counter-productive to maintaining the integrity of a digital trade ecosystem.

REFERENCES

Aaronson, Susan and Maxim, Rob (2013). "Data Protection and Digital Trade in the Wake of NSA Revelations." http://elliott.gwu.edu/sites/elliott.gwu.edu/files/downloads/research/aaronson-Data%20Protection%20and%20Digital%20Trade%20in%20the%20Wake%20of%20the%20NSA%20Revelations.pdf

AmCham China (2015). "Protecting Data Flows in the US-China Bilateral Investment Treaty." http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization

Apple Press Info (23 February 2015). "Apple to Invest €1.7 Billion in New European Data Centres." https://www.apple.com/ie/pr/library/2015/02/23Apple-to-Invest-1-7-Billion-in-New-European-Data-Centres.html

Asia Internet Coalition (2014). "Coalition for cross-border data flows." http://www.asiainternetcoalition.org/wp-content/uploads/2014/10/Data-Resource-Paper-July-3.pdf

Atkinson, Robert (2010). "Time to end rampant mercantilism." G8G20 Summit 2010. http://www.itif.org/files/G8G20_RAtkinson.pdf

Bajoria, Jayshree (5 June 2014). "India's Snooping," *Wall Street Journal (India)*. http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snooping-and-snowden/

Bauer, Matthias *et al* (2013). "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce." https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_ Final_Revised_lr.pdf

Bauer, Matthias *et al* (2014). "The Costs of Data Localization: Friendly Fire on Economic Recovery." *ECIPE Occasion Paper no.* 3/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

Bauer, Matthias *et al*. (2015). "Data localization in Russia: a self-imposed sanction." *ECIPE Policy Brief* no. 6/2015. http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf

BBC News (16 October 2014). "Huwaei boss says US ban not very important."http://www.bbc.com/news/business-29620442#

Bowman, Catherine (27 August 2015). "A Primer on Russia's New Data Localization Law (blogpost)." *Privacy Law Blog. http://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/*

Castro, Daniel and Mcquinn, Alan (2015). "Cross-Border Data Flows Enable Growth in All Industries." http://www2.itif.org/2015-cross-border-data-flows.pdf

Chander, Anupam and Le, Uyen (2015). "Data Nationalism." *Emory Law Journal* 64, no. 1: 677-739. http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html

Chander, Anupam (2009). "Trade 2.0." UC Davis Legal Studies Research Paper Series Research Paper No. 173. http://www.law.uchicago.edu/files/files/465-chander-trade.pdf

Chander, Anupam and Le, Uyen (2014). "Breaking the Web: the Global Internet v/s Data Localization." *UC Davis Legal Studies Research Paper Series Research Paper* No. 378. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858

Crawford, Gail (26 March 2015), "Snowden's legacy: Safe harbour under fire at the CJEU (blogpost)." http://www.globalprivacyblog.com/privacy/snowdens-legacy-safe-harbor-under-fire-at-the-cjeu/

Cushman and Wakefield (2013). "Data Centre Risk Index." http://www.cushmanwakefield.com/~/media/global-reports/data-centre-risk-index-2013.pdf

Dani Rodrik (2013). "The new mercantilist challenge," http://www.project- syndicate.org/commentary/the-return-of-mercantilism-by-dani-rodrik

Data Centre Knowledge (21 July 2015). "Firms rethink Russian data strategy." http://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes/

Dhont, Jan and Woodcock, Katherine (2015). "Data localization requirements: Growing trends and impact for company compliance," *Corporate and Ethics Professional*. http://www.lorenz- law.com/wp-content/uploads/Data-localization-requirements-Growing-trends-and-impact-of- compnay-compliance1.pdf

Donnan, Shawn (14 August 2014). "Digital trade: Data protectionism." *The Financial Times*. http://www.ft.com/intl/cms/s/0/93acdbf4-0e9b-11e4-ae0e- 00144feabdc0.html#axzz3WD30VpD4

Donohue, Laura (2015). "High Technology, Consumer privacy and US National Security," *Georgetown Law Faculty Publications and Other Works.* Paper 1457. http://scholarship.law.georgetown.edu/facpub/1457/

Drezner, Daniel (20 June 2012). "A most unusual foreign policy poll." *Foreign Policy*. http://foreignpolicy.com/2012/06/20/a-most-unusual-foreign-policy-poll/

eBay Inc. (2015). "Commerce 3.0: Enabling Small and Medium Enterprises." http://www.ebaymainstreet.com/sites/default/files/asean_commerce_3_0_final_1.pdf

Ezell, Stephen (2012). "The Benefits of ITA Expansion for Developing Countries." http://www2.itif.org/2012-benefits-ita-developing-countries.pdf

Ezell, Stephen (2014). "Safeguarding Digital Trade is vital to ensure thriving innovation economy," *Bridges* no. 39. http://ostaustria.org/bridges-magazine/item/8177-safeguarding-digital-trade-is- vital-to-ensuring-a-thriving-global-innovation-economy?tmpl=component&print=1

Ezell, Stephen and Atkinson, Robert (2010). "The Good, the Bad, the Ugly, and the Self-Destructive of Innovation Policy ." http://www.itif.org/files/2010-good-bad-ugly.pdf

Ezell, Stephen *et al.* (2013). "Localization barriers to global trade: threat to the global economy."http://www.itif.org/publications/localization-barriers-trade-threat-global-innovation- economy

Gilpin, Robert (2001). *Global Political Economy.* New Jersey: Princeton University Press.

Grampp, William (1952). "The Liberal Elements in English mercantilism." *The Quarterly Journal of Economics* 66, no. 4: 465-501.

Heidt, Franz (2015). "The Harms of Forced Data Localization," https://www.leviathansecurity.com/blog/the-harms-of-forced-data-localization/

Hill, Jonah (2014). "The Growth of Data Localization Post-Snowden." *Lawfare Research Paper Series* 2, no. 3:1-40.

Information Technology Industry Council (15 October 2014). "ITI Joins Broad International Coalition Urging TPP Negotiations Ensure Robust Cross-Border Data Flow Provisions."http://www.itic.org/news-events/news-releases/iti-joins-broad-international-coalition-urging-tpp-negotiations-ensure-robust-cross-border-data-flow-provisions

Irwin, Douglas (1991). "Mercantilism as a strategic trade policy." *The Journal of Political Economy* 99, no. 6: 1296-1314.

ITI, JEITA and Digital Europe (2014). "The Tokyo Resolution on Combatting Data Localization Requirements." http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=841&PortalId=0&TabId=353

Kehl, Danielle *et al* (2014). "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cyber security." http://newamerica.net/publications/policy/surveillance_costs_the_nsas_impact_on_the_economy _internet_freedom_cybersecurity

Kong, Lingjie (2010). "Data Protection and Transborder Data Flow in the European and Global Context." *European Journal of International Law* 21, no. 2: 441-56.

Krasner, Stephen (1976). "State power and the structure of international trade", *World Politics*, pp. 317-347 http://www.indiana.edu/ğradipe/docs/krasner.pdf

Kurochkin, Dmirt *et al* (2015). "Russia's New Server Localization Law: Implications for foreign companies." *World Data Protection Report* 15, no. 2: 1-3. https://www.dechert.com/files/Uploads/Documents/Bloomberg%20-%20Russia%20New%20Server%20Localization%20Law%20-%20Dechert%20LLP%20-%20February%202015.pdf

Lee-Makiyama, Hosuk (2013). "European leaders show leave data flows open." http://www.euractiv.com/infosociety/european-leaders-leave-data-flow-analysis-530785

Lee-Makiyama, Hosuk (2015). "Data localization requirement in Russia." http://www.ecipe.org/blog/data-localisation-russia/

Livemint (30 July 2015). "India, US on a collision course over e-commerce, IP norms." http://www.livemint.com/Politics/FNMRmLJElPC6zwA7K4NZQL/India-US-on-a-collision-course-over-ecommerce-IP-norms.html

McKinsey Global Institute (2014). "Global flows in a digital age." http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age

Milberg, Sandra *et al*. (2000). "Information Privacy: Corporate Management and National Regulation." *Organizational Science* 11, no. 1: 35-57.

Mulvenon, James and Abraham Denmark (2010). "Contested Commons: The Future of American Power in a Multipolar World." http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

NPR (15 June 2015). "Brazil's Cybercrime Free-For-All: Many Scams and Little Punishment." http://www.npr.org/sections/parallels/2015/06/15/414622197/brazils-cybercrime-free-for-all-many-scams-and-little-punishment

Nye, Joseph. (2014). "The Regime Complex for Global Cyber Activities." https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Office of the United States Trade Representative (2015). "Trans-Pacific Partnership: Summary of US Objectives." https://ustr.gov/tpp/Summary-of-US-objectives

Panel Discussions (30 July 2015). "Trade Agreement and Data Flows: Safeguarding the EU Data Protection Standards." http://europe-liberte-securite-justice.org/2015/07/30/trade-agreements-and-data-flows-safeguarding-the-eu-data-protection-standards/

Post, Robert (2001). "Three concepts of privacy." *Faculty Scholarship Series*. Paper 185. http://digitalcommons.law.yale.edu/fss_papers/185

Reuters (US Edition) (5 August 2015). "EU close to sealing deal with US on data sharing." http://www.reuters.com/article/2015/08/05/us-usa-eu-data-idUSKCN0QA1XB20150805

Robert, Atkinson (2014). "The Rise of Innovation Mercantilism." *International Economy* 28, no. 2: 30-32 and 55-56.

Rubin, Ryan (2015). "Companies should prepare for EU's forthcoming data protection regulation." http://www.euractiv.com/sections/infosociety/companies-should-prepare-eus-forthcoming- data-protection-regulation-312487

Svantesson, Dan (2010). "Privacy, the Internet and transborder data flows - An Australian perspective," *Masaryk University journal of law and technology* 4, no.1: 1-20.

The Economist (23 August 2013). "What was mercantilism?." http://www.economist.com/blogs/freeexchange/2013/08/economic-history

The Economist (7 May 2015). " Spicing up growth." http://www.economist.com/news/finance-and-economics/21650586-bad-policy-much-bad-infrastructure-holding-indonesia-back-spicing-up

The Economist (7 May 2015a). "Jokowi's to-do list." http://www.economist.com/news/leaders/21650544-indonesias-president-should-ditch-his-economic-nationalismand-if-necessary-his-party-jokowis

The Guardian (8 July 2015). "FBI chief wants 'backdoor access' to encrypted communications to fight Isis." http://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis

The Irish Times, "Ireland's Data Centre Boom to Continue," March 5, 2015, http://www.irishtimes.com/business/technology/ireland-s-data-centre-boom-set-to-continue-1.2126081

The Wall Street Journal (13 November 2013). "Brazil legislators bear down on Internet Bill." http://www.wsj.com/articles/SB10001424052702304868404579194290325348688

UNCTAD (2013). "Information Economy Report." http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf

US Chamber of Commerce (19 May 2015). "Safeguard Cross-border data flows." https://www.uschamber.com/issue-brief/safeguard-cross-border-data-flows

US Chamber of Commerce and Hunton & Williams (2014). "Business without borders." https://www.huntonprivacyblog.com/files/2014/05/021384_BusinessWOBorders_final.pdf

Van der Marel, Erik (2015). "Disentangling the flows of data: Inside or Outside of the Multinational Company?." http://www.ecipe.org/publications/flows-data-inside-outside-multinational-company/?chapter=all

Walter, Andrew (1996). "Adam Smith and the Liberal Tradition in International Relations." *Review of International Studies* 22, no. 1: 5-28.

ZD Net (2 April 2013), "Is it better to build or outsource a data center?" http://www.zdnet.com/article/is-it- better-to-own-or-outsource-your-data-center/