Challenges relating to cross border flows of data

Chamindi Ekanayake[1#]
[1]*Attorney-at-Law, Senior Associate - Nithya Partners*
[#]*For correspondence <chamekanayake@yahoo.com>*

Abstract— Developments in technology are gradually changing the manner in which trade conducted throughout centuries. Trade of goods and services are gradually been replaced by trade of data across borders. Taking into consideration the value given for data today it can be considered the new oil in the 21st century. There are number of challenges when data is being transferred across borders. This includes protection of personal data and privacy, combating cybercrimes, protection of intellectual property. In addition, there is a great divergence between countries on free flow of cross border data. Some jurisdictions favour data protection and promotion of privacy over free flows of data whereas the others promote cross border flows of data for the promotion of international trade. The objective of this paper is to identify the given challenges and to discuss the measures that have taken by the countries to overcome such challenges and to promote transfer of data. As the research Methodology are online study done on international treaties such as OECD Guidelines, EU Regulations on data protection, APEC framework, statutes and decided cases from other jurisdictions, published articles on cross border data transfers, privacy and data protection and the challenges relating thereto.

Keywords—**Cross Border Data Flows, Privacy, Data Protection**

I. INTRODUCTION

Free flows of data across border has been identified as a market driving force in the 21st century. But there are number of limitation and restrictions which hamper such free flows of data. This paper identifies the given challenges relating to cross border data transfers and discuss the mitigatory measures taken by countries to reduce the impact of such restrictions.

Part 1 of this paper shall examine the manner in which flows of data is gradually replacing the traditional mode of international trade and the growing importance given to data today.

Part 2 will discuss the checks and balances placed by the governments to protect and promote privacy and data protection, prevention of computer crimes etc. which inadvertently impose limitations and restrictions on free flows of data.

Part 3 of the paper will discuss firstly the international and regional approaches towards promoting cross border data transfers followed by a discussion on national legislations.

Part 4 will discuss the mitigatory measures taken by jurisdictions to remedy the disparities and to reach a consensus when transferring data across borders.

Part 5 will provide the concluding remarks.

II. PART I- DATA – THE NEW OIL

In the 21st century the traditional trade of goods and services is fast being replaced by flows of data across boundaries. Such data flows are enabled with the assistance of the developments in the internet and information technology (Meltzer 2014). Needless to state that in the past decade internet has changed all aspects of everyday life and today it has become a vital component of international trade. Internet connectivity and increase in trade seems to go hand in hand as between 1996-2011 there had been a 10% increase in broadband penetration and this has raised annual 1.35% increase in GDP for developing countries and 1.19% in developed countries (IHRB, 2016).

Internet has introduced new modalities of conducting businesses. Electronic platforms such as Amazon, Alibaba, E-bay has made international trade accessible to everyone. Approximately 12% of global goods trade today is conducted via international e-commerce (Mckinsey Report, 2016). For start-ups and SME's the cost of conducting business has been greatly reduced by such developments. US ITC has estimated that the internet has reduced 26% of the trade costs on average (US ITC, 2014). In addition, internet has changed the manner in which traditional businesses are conducted across border. Today it is possible to maintain the company headquarters in one jurisdiction, manufacturing in another and to conduct business real time with marketing teams joining from different jurisdictions. According to research an estimate of 75% of the internet's benefit is being captured by companies in traditional industries (Mckinsey Report, 2016). With digitalization is the new mode of globalization it has been estimated that in 2012, 61% of total US service exports and that 53% of the US imports were digitally delivered (Meltzer 2014).

With digitalization of trade, the new oil in the 21st century undoubtedly is data (http://fortune.com/2016). According to McKinsey Report (2016) cross border data flows now generate more economic value than traditional flows of traded goods. Therefore, with the growth of importance heavily weighting upon data, free flows of such data across boundaries becomes a crucial aspect for international trade.

Recent developments in related technologies have greatly assisted enterprises and government alike. Cloud computing, big data and internet of things (IOT) have been recognized as recent developments relating to information technology. Cloud computing has been defined by the National Institute of Standards and Technology as a pay per use model for enabling available, convenient, on-demand network access to a shared pool of configurable computer services such as networks, servers, storage, applications. Cloud computing is appealing to individuals and businesses alike for economic feasibility. It has been estimated that 59% of the global internet users will use cloud computing by 2020 (Cisco's Global Cloud Index, 2016).

Big data is the processing of large quantum of data by companies with special expertise to provide required results for enterprises and other institutions (Sivarajah, 2017). Big data provides enterprises with necessary business insights. It has been estimated that businesses that have harnessed big data have seen a 60% operating margins in their businesses (McKinsey & Company, 2011).

IOT is the networking of devices, vehicles, buildings and other items to collect and exchange data (https://www.exact.com). Therefore, in addition to the computers and the smart phones to transfer data the new advances allow other appliances to engage in data collection and exchange which reflects the revolution that is taking shape in the near future. It is estimated that by 2020 there will be 26 Billion connected devices (http://www.gartner.com). With the world slowly moving towards smart cities and smart countries the question is how freely the data will be transferred across borders.

III. PART II - CHALLENGES ON CROSS BORDER TRANSFER OF DATA

Although it is emphasized that free flows of cross border data should be allowed, there are number of restrictions and limitations in relation to free flows of cross border data. Some of them are listed as follows;

A. Privacy and data protection

By 2013, 99 countries have introduced some form of privacy and data protection laws that restrict the use of personal data (Greenleaf, 2013). Many countries have restricted the transfer of data cross border as they are concerned that the other countries may not have adequate protection for data. Setting up barriers to transfer data across borders is referred to as data localization (Ezell, 2013). For example, section 26 (1) of the Personal Data Protection Act 2012 (PPDA) of Singapore states that an organization must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the Act to ensure that organizations provide a standard of protection to the personal data that was transferred so that it is compatible with the protection provided under the PPDA.

In addition, countries such Russia, China, Vietnam have legislations which insist that personal data of its citizens be kept on local servers. Needless to state that such localization measures by countries hamper cross border transfers of data.

B. Cybercrimes

Initially the main concern on cybercrimes was relating to unauthorised access of personal information. But with the evolution of technology, increased connectivity magnified the cybercrimes and today they can take the form of copyright infringements, child phonography, global fraudulent financial schemes or cyber terrorism. (Clough, 2010)

Budapest Convention on Cyber Crimes has recognized following as computer related crimes. Illegal access, illegal interception, data and system interferences, misuse of devices, fraud and forgery using computers, child phonography and intellectual property rights violations. Many countries including Sri Lanka are party to the said convention and many have national legislations in place on cybercrimes.

Cybercrimes are a challenge to cross border transfer of data. Incidents such as computer related frauds create certain cautiousness among general public when their data is being processed in other countries. As a result, increase cybercrimes can hamper free flows of data across borders.

C. Intellectual Property Rights

Although the internet provides hosts of opportunities, on the other hand it is deemed a nightmare for patrolling for intellectual property rights. Today where everything is available with a click of a button protection of copyrights, trademarks, patents, industrial designs and trade secrets have become a daunting task.

For example, issues such as BitTorrenting, where large files are being shared over peer to peer networks for the viewing of pirated movies and songs, is a growing

concern. In the case filed against Artem Vaulin, the proprietor of Kickass Torrents it was alleged that his site was the 69th most visited site in the internet and had 50 Million unique visitors every month (http://fortune.com/2016). This will mean Millions of dollars in losses for genuine copyright holders. Therefore, many legislations are available today to combat such intellectual property related crimes.

D. National Security

In the 21st century national security can be challenged by internet. It has been noted that data in relation to national security is being defined as important data. This is an effort to create a new data criteria and moving beyond the traditional criteria of personal data and business data. Countries require an assessment of important data before them being transferred beyond borders. In the big data era many multinational companies have vast sources of data and any infringements in such data not only have an impact on personal information but also on national security as well (Hong, 2017). Therefore, in many data protection legislations, national security is being mentioned as an exceptional situation where data protections laws will not be applicable. But in relation to cross border transfer of data, data which have an implication on national security can be restricted by legislations.

IV. PART III - OVERVIEW OF LAWS AND REGULATIONS RELATING TO TRANS-BORDER FLOWS OF DATA

A. International Regulations

In recognizing the importance of cross border data flows there are number of initiatives taken by international and regional organizations.

What is noted is there is a divergence in the treatment of cross border data by two main international statutes on the subject namely the OECD Guidelines on the protection of privacy and trans-border flows of personal data (OECD Guidelines) which was introduced in 1980 and Convention for the protection of individuals with regard to automatic processing of personal data which was introduced by the Council of Europe in 1981 (Convention 108).

The OECD Guidelines highlight the importance of protecting personal data but at the same time has emphasized that restriction on data flows will hamper trade. In relation to cross border data transfers the following guidelines have been introduced by the OECD;

Article 15 – Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

Article 16 – Member countries should take all reasonable steps to ensure that trans-border flows of personal data are uninterrupted and secure.

Article 17 – A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe the OECD Guidelines or where re-export of such data would circumvent its domestic privacy legislations. A Member country may also impose restrictions in relation to certain categories of personal data for which specific regulations are available in the home country and when no equivalent protections are provided by the other Member country.

It is to be noted that many jurisdictions for example New Zealand Privacy Act 1993; UK Data Protection Act 1998; The South Africa Protection of Personal Information Act No. 4 of 2013 have used the principles set out by the OECD Guidelines.

On the other hand, Convention 108 is the first ever binding international instrument on protection of personal data and cross border data transfers (Unver, 2016). Article 12 (2) of the Convention states that "a Party shall not for the sole purpose of the protection of privacy, prohibit trans-border flows of personal data going to the territory of another party." Article 12(3) provides the exemption for the general rule. i.e. when specific categories of personal data are being governed by special regulations such personal data shall not be transferred unless the other party does not provide adequate protection.

The European Union Regulation 2016/679 relating to the protection of natural persons with regard to the processing of personal data and on the free movement of such data is the latest Regulation in relation to cross border data transfers applicable to the European Union. According to Article 45 transfer of data to a third country or an international organization may take place when the European Commission decides that the particular country has "adequate" privacy protections. So far only 11 countries have been recognized outside the EU as having adequate protection (http://ec.europa.eu/).

Therefore, European Union being one of the biggest global traders have stricter regulations on personal data whereas the approach taken by USA is somewhat different and is recognized by EU as not having adequate data protection (NBT, 2014). As a result, the European Commission in 2000 approved EU-US Safe Harbour Framework as a special "adequate" protection mechanism. According to the said Framework US Companies can self-certify that they comply with the Safe Harbour principles and thereby qualify under EU regulations as "adequate." But Safe Harbour principles were recently declared invalid by the European Court of Justice (Schrems vs. Data Protection Commissioner, C-362/14) and in 2016 this was replaced by the EU-US Privacy Shield.

The Asia-Pacific Economic Corporation (APEC) has introduced a Privacy Framework. APEC has introduced number of principles such as preventing harm, notice, collection limitation principle whereby it is expected that member countries to create their own privacy rules in consistent with the principles recognized.

But lack of consensus among the international treaties is a grave concern. When different countries and regions adopt different approaches for cross border data transfers this creates a negative impact on the transfer of data.

B. National

As there is no model law available national approaches too vary on cross border data flows. Some countries have used the "omnibus approach" where they have introduced one overarching law that regulates data protection and cross border data flows e.g. South African Protection of Personal Information Act No. 4 of 2013 (POPI), EU data protection regulations.

On the other hand, countries such as India and the USA have used the "sectoral approach" where different sectors such as health are regulated separately (NBT, 2014). Quite contrary to these approaches some countries such as Sri Lanka do not contain any legislations at all.

V. PART IV – Migratory Measures

Since there is no global consensus on cross border transfers there are number of mitigatory steps taken by international organizations as well as countries to enable cross borer transfers (Meltzer 2014);

1. Adequacy approach – Followed by the EU this assesses whether the other jurisdiction provides sufficient degree of protection for personal data in the event of a cross border transfer. For example, the Privacy Shield which was discussed above.

2. Binding Corporate Rules (BCR) – According to Article 47 of the EU Regulations, this is a set of internal rules adopted by a multinational company which defines their global policy on transfer of personal data within the group of companies but physically located at different countries. This internal standard has been recognized as a method which prevents data infringements in countries outside the EU and avoiding the need for a contract every time data is being transferred. (http://ec.europa.eu). In EU BCRs needs to be approved by the data protection authority in each member state. Similar provisions are available on national legislations i.e. South Africa, POPI.

3. Model Contract Clauses (MCC) – Used by EU this approach allows a third party which uses a specific model words in their contract to provide adequate protection for the data that is being transferred. EU has developed two types of standard clauses which govern both data controller to data controller and data controller to data processor relationship. MCCs are more popular but on the other hand this may be cumbersome for multinational companies as they need to have data processing agreements in place with each and every entity with whom they will be exchanging data. (Bloom and Royal, 2015)

4. Consent – Many countries would require the consent of the data subject for the transfer of personal data to another jurisdiction. In Belgium according to Law on the protection of privacy in relation to the processing of personal data, transfer of personal data to countries which have not been recognized as providing adequate protection is in principle prohibited (Article 21). But there are certain exemptions and one such exemptions is that the data subject has given his unambiguous consent to the proposed transfer (Article 22).

5. Contracting purposes – Personal data transfer is allowed in an instance where performance of a contract between the data subject and a third party.

V. PART IV - Conclusion

What is to be noted is that although it is evident that free flows of data promote trade and is beneficial for individuals and for companies alike but lack of consensus between the legal approaches seems to create issues.

What is noteworthy is that there is no model law for the governess of cross border transfer of data. Many legislations have opted for the EU based laws relating to data protectionism thereby restricting flows of data and on the other hand some countries have opted for sectoral approach by bringing in different laws to govern different sectors. All in all, this has an implication on businesses as they will have to comply with different sets of legislations in each jurisdiction that they conduct business. On the other hand, some countries such as Sri Lanka do not have specific legislations on data protection and cross border data flows. This approach will definitely isolate the country whereby other countries will not transfer data to countries such as Sri Lanka for processing as they do not provide the adequate safeguards that is required. Therefore, when trying to rely on knowledge economy such lacunas in the domestic laws should be remedied if the country is to reap benefits from the new digitalized world economy.

So what is required today is a Model law which strikes a balance between the privacy of individuals and data protection at the same time which promotes international trade.

References

Cisco's Global Cloud Index, forecast and methodology, 2015-2020, White Paper, 2016

Graham Greenleaf, Local data privacy laws, 99 countries and counting Privacy laws and Business Report issue 123, 2013

Yanqing Hong, The cross border data flows security assessment: an important part of protecting China's basic strategic resources, working paper, June 2017

Institute of Human Rights and Business (IHRB), No trade off: How the free flow of data enhances trade and human rights, June 2016

Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2010

Joshua Paul Meltzer, The Internet, Cross-Border Data Flows and International Trade, Asia and Pacific Policy Studies, 2014

Katia Bloom and K Royal, Transferring Personal Data out of the European Union, which export solution best fits your needs, ACC Docket, June 2015

National Board of Trade, No transfer; no trade; the importance of cross border data transfers for companies based in Sweden, January 2014

Mckinsey Global Institute, Digital Globalization: the new era of global flows, 2016

McKinsey & Company, Big data: the next frontier for innovation, competition and productivity, 2011

Pedro Asensio, Internet Intermediaries and the Law Applicable to Intellectual Property Infringements

Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, Localization Barriers to Trade: Threat to the Global Innovation Economy (Information Technology and Innovation Foundation, September 2013)

United States International Trade Commission, Digital Trade in the US and global economies, August 2014

Uthayasankar Sivaraja, Muhammad Mustafa Kamal, Zahir Irani, Vishanth Weerakkody, Critical Analysis of Big Data Challenge, Journal of Business Research, 2016

Ms. Chamindi Ekanayake has obtained her LL.B (Hons), LL.M and MBA (Finance) from the University of Colombo. She currently works as a Senior Associate at Nithya Partners, Attorneys-at-Law