DATA PROTECTION LAWS: INCORPORATION OR REJECTION IN THE INDIAN CONTEXT

Written by ***Anoushka Borker***

2nd Year BA LLB Student, School of Law, Christ (deemed to be university)

ABSTRACT

Technological advancements have produced numerous threats to human rights. One such threat is caused due to increasing use of computers in the contemporary society. Governmental organisations, websites and various other firms are now able to record a vast amount of personal information in the digital data banks. Individuals may suffer when information contained in these portals is inaccurate, inappropriate or is disclosed for an unauthorized purpose. In this paper I address the issues related to data protection and storage in digital data banks. In this paper I shall bring about a comparative analysis amongst a sample of countries i.e. Australia, Brazil, Canada, China, France, Germany, Indonesia, Russia, South Korea and India on the basis of the data protection regulations prevalent in these respective countries. The countries in the above sample differ from one – another in terms of their levels of data transfer regulations and enforcement mechanisms. The primary focus in this paper is on the European Union General Data Protection Regulations as the Article 45 of the above - mentioned document provides for an adequacy test for transfer of personal data to a third country. This test stipulates that personal data of EU subjects to non-EEA countries is not permitted unless those countries are deemed to have an "adequate" level of data protection. I shall also throw light upon the current state of data security in India, with special emphasis on the Information Technology Act and various other cyber security laws. Through the study of the above mentioned data, one can comprehend the applicability of such regulations to the Indian context. This paper also proposes certain recommendations in the field of data privacy. To conclude I would say that the issue of cross border flow of data is even more expansive than the jurisdictions we identify.

INTRODUCTION

> *"Data needs to move to create value. Data sitting alone on a server is like money hidden under a mattress. It is safe and secure, but largely stagnant and underutilized."*[1]

Anupam Chander in his article entitled "Data Nationalism"[2] depicts the imagination of an Internet where data must stop at national borders, examined to see whether it is allowed to leave the country and possibly taxed when it does. He warns that while it may sound fanciful, this is precisely the impact of various measures undertaken or planned by many nations to curtail the flow of data outside their borders.[3] According to him, we must insist on 'data protection' without '*data protectionism'*. In order for companies to do business, be innovative, and stay competitive in global markets, they need to be able to send not only goods, capital, and competence (of people) across borders, but also data. At present, almost half of the global services trade is information and communication technologies-enabled, including cross-border data flow.[4] However, Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are erecting borders in cyberspace, disintegrating the World Wide Web.[5] In April 2011, the Indian Ministry of Communications and Technology published privacy rules implementing certain provisions of the Information Technology Act of 2000.[6] The "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules" limit the transfer of "sensitive personal data or information" abroad to two cases—when "necessary" or when the data subject consents to the transfer abroad.[7] The European Union's 1995 Data Protection Directive recognized that the

[1] Kommerskollegium, National Board of Trade, 'No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden' (2014), available at http://unctad.org/meetings/en/Contribution/dtl_ict4d2016c01_Kommerskollegium_en.pdf (last accessed on 28.06.2018)

[2] Anupam Chander ; Uyên P. Le, Data Nationalism, available at http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf (last accessed on 28.06.2018)

[3] *Ibid*

[4] UNCTAD (2009). For the U.S.A., it is 60 per cent (Borga and Koncz-Bruner, 2012) while it is slightly below 50 per cent for Sweden (own calculation).

[5] Supra note 2

[6] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[7] Rule 7, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

free flow of data across borders was necessary to commerce.[8] Accordingly, it allowed data to be sent outside the European Union (or the European Free Trade Association states) if it were protected adequately either by local law or by contractual arrangement with the foreign company.[i]

ISSUES CONCERNING CROSS BORDER TRANSFER OF DATA

Most businesses that wish to transfer personal information currently use one of three options: obtain the consent of the individual concerned; establish a contract between the entities exchanging the information; or if transferring from the EU, limit data flows to jurisdictions where there is an "adequacy" finding such as the U.S. Safe Harbor regime.[9] In some situations, however, organizations may be unable to rely on the use of the three options above to make their international data transfers legal. For example, many banks function internationally through branches rather than through separate legal entities; therefore, contracts generally cannot be used when the same legal entity would be on both sides of the contract.

NEED FOR CROSS-BORDER FLOW OF DATA

Cross-border data flows are crucial for the day-to-day operations of Companies and moving data is about the ability to control and make operations more efficient. It is important to underline that data transfer is not confined to high-tech companies in the IT and communication sectors.[10] Rather data is essential in all economic sectors. It could be argued that data transfers are relatively more important for small companies than large.[11] This is due to the fact that small

[8] See Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 36–37 [hereinafter Council Directive] ("Whereas cross-border flows of personal data are necessary to the expansion of international trade . . . .").

[9] See Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 56,534 (Sept. 19, 2000); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (Jul. 24, 2000) .available at, http:// www.export.gov/safeharbor/doc_safeharbor_index.asp (last accessed on 28.06.2018).

[10]

[11] Supra note 1

companies have fewer resources to handle barriers and, additionally, using digital solutions like cloud computing can free relatively more resources for these companies.

Cross-border data flows have also been a driving force behind the emergence of so-called global value chains (GVCs) in which businesses' operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production.[12]

Barriers to data flows, whether due to privacy and cyber-security concerns, law enforcement, or digital mercantilism—affect a growing share of economic activity, not to mention a key area of competitiveness, as data is increasingly important to both modern and traditional sectors of the economy. It has been suggested that there is a need to value foundational role that data plays in today's economy.[13]

Unnecessary barriers to cross border data flows create considerable obstacles to global trade. Ultimately, without the free flow of data consumers and businesses are unable to access valuable digital services. Small and medium-sized enterprises (hereinafter 'SMEs'), which greatly benefit from digital trade, can be disproportionately affected by barriers that are created. Many times, SMEs do not have the resources to bear the costs of entering into a new market, restricting their global reach. Providing strong rules to protect cross-border data flows is vital for SMEs, consumers, and multi-national businesses.[14]

ADDITIONAL CONSENT AND PRIVACY

Special consent required for exporting data suggests that data sent to another country is, by that act, less safe—thus requiring special knowledge and approval of the data subject.[15] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules do not make it clear how consent for onward transfer from the

[12] Supra note 1
[13] Nigel Cory, 'Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions' (April,2017), available at http://www2.itif.org/2017-usitc-global-digital-trade.pdf, (last accessed on 28.06.2018)
[14] See https://servicescoalition.org/services-issues/digital-issues/cross-border-data-flows (last accessed on 28.06.2018)
[15] Supra note 2

information collector to the information processor is to be obtained. When it comes to collecting the personal information in the first instance, the rules require consent

It has been pointed out that since consent for offshore transfer can be a significant practical hurdle, American critics of outsourcing to India have sought to impose a consent requirement before consumer information can be sent outside the United States. As drafted, the Indian law undermines the goal of enabling outsourcing of data to India—by requiring American companies to obtain the consent of individuals before passing their information to India.[16]

As mentioned above, organizations can legitimize the transfer of personal information from one country to another by obtaining the consent of the individual to transfer his or her personal information. In most EU Member States, for example, consent to transfer personal information to a country that has not been deemed adequate by the EU would need to be affirmative (opt-in) consent. Similarly, affirmative consent is usually required in countries such as Argentina, Korea, Mauritius, and the U.A.E. (DIFC). In other countries such as Australia and Canada, opt-out consent may be sufficient. Regardless of the form of consent required, almost all jurisdictions require that such consent be informed and as such, notice would need to be provided.

As the amount of personal data generated grows, so do concerns from individuals about how their personal data is being used. This is one reason why governments need to restrict the free flow of information across borders. Such restriction can take the form of legal requirements to store data within a country's borders and regulations that restrict the ability to move and process personal data across borders.

REDUCTION IN COSTS AND INCREASE IN INNOVATION

A central problem for companies is how data regulation, especially restrictions on moving data to third countries, could entail missed business opportunities by increasing costs and inducing delays, making companies' prices unattractive or making products late to market. This also affects innovation.

[16] Supra note 2

INTERNATIONAL PRACTICES

In order to determine whether cross-border transfers of data can be done, various countries have their theories and models like, the EU has three mechanisms to regulate such transfers. These include the "adequacy test" as set out under Article 45 of the EU GDPR[17], Model Contractual Clauses [18]and Binding Corporate Rules[19]. Additionally, cross-border transfers of data between the EU and the US can also be done by way of the Privacy Shield Framework. Each of these will be discussed in greater detail below. In this part, various sets of data protection and transfer laws that are applicable across the globe have been analysed.

India

Rule 7 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 stipulates the permission to transfer data across borders in the following words:

> *"A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer."*

[17]Art. 45, European Union General Data Protection Regulation, available at https://gdpr-info.eu/art-45-gdpr/ (last accessed on 28.06.2018)
[18]Model Contracts for the Transfer of Personal Data to Third Countries, available at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last accessed on 28.06.2018)
[19]*Ibid*

European Union General Data Protection Regulation

Article 45 of the EU GDPR[20] provides for an adequacy test for transfer of personal data to a third country. This test stipulates that personal data of EU subjects to non-EEA countries is not permitted unless those countries are deemed to have an "adequate" level of data protection. While making this decision, the EU Information Commission will examine whether the country to which data is intended to be transferred has data protection rules in place; whether they have effective and enforceable data protection rights and their effective administration; whether independent data protection supervisory authorities exist, who are vested with the power to ensure compliance; and finally, whether the country in question has entered into any international commitments with regard to data protection.

These safeguards do not involve the execution of model contractual clauses between exporters and importers, or developing binding corporate rules.

Under this provision, when assessing "the adequacy of the level of protection", the Commission will take account of "rules for the onward transfer of personal data to another third country or international organization." [21] Further, this article allows transfers of personal data to third countries which do not have adequate data protection without the appropriate safeguards for the transfers as listed in Article 49,[22] if such transfer is "necessary for important reasons of public interest."

Binding Corporate Rules

Binding Corporate Rules (BCR) are internal rules (such as codes of conduct) which are adopted by multi-national group of companies. BCRs define the global policy of multi-national group of companies with regard to the international transfers of personal data within the same corporate group, to entities located in countries, which do not provide an adequate level of protection. Multinational companies use BCRs in order to adduce adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals within the meaning of Article 47 of the EU GDPR.

[20] *Supra*, note 7
[21] Article 45 (2) (a), European Union General Data Protection Regulation.
[22] Article 49, European Union General Data Protection Regulation.

Model Contractual Clauses

The Information Commission has the power to decide that certain standard contractual clauses offer sufficient safeguards with respect data protection while undertaking transfer of data to non-EU/EEA countries. As of date, the Commission has issued two sets of standard contractual clauses: one for transfers from data controllers to data controllers established outside the EU/EEA; and one set for the transfer to processors established outside the EU/EEA. Transfers of data made under these contracts are deemed to be protected under the EU data protection law. Since it is often difficult for stakeholders to comply with the 'adequate level' of protection for cross-border data transfers, alternatives such as Model Contract Clauses may play a crucial role in practice. The use of these alternatives should be facilitated for data controllers in any Member State.

Privacy Shield

There are two Privacy Shield Frameworks:

(i) the EU-US Privacy Shield Framework, which is deemed adequate by the European Commission to enable data transfers between the EU and the US; and

(ii) The Swiss-US Privacy Shield Framework, which is deemed adequate by the EU to enable data transfers between Switzerland and the US. In order to join either framework, US organisations wishing to engage in data transfers must self-certify their adequacy to the Department of Commerce and publicly commit to the framework requirements.

United Kingdom

Before BREXIT, the United Kingdom was a part of the EEA. On leaving the EU, the UK would become a "third country". The United Kingdom Government has recognized the need for a framework to ensure that data transfers between the UK and non-EU countries can continue securely and efficiently.[23] The Government has declared its desire to establish an enhanced relationship between the UK and EU for the transfer of personal data following the UK's exit from the EU. This would be based on the existing adequacy model.

[23]UK Finance, 'Data protection and transfer', available at https://www.ukfinance.org.uk/wp-content/uploads/2017/09/BQB5-Data-protection-and-transfer-v2.pdf (last accessed on 28.06.2018)

South Africa

The South African Protection of Personal Information Act, 2013 provides that a "responsible party" in South Africa cannot transfer personal information about a data subject to a third party in a foreign country, unless the recipient is subject to a law, binding corporate rules or any other binding agreement which provides substantially similar conditions for lawful processing of personal information relating to a data subject. A "responsible party" can also transfer personal information about a data subject to a third party in a foreign country if the following conditions are met:

(i) if the data subject consents to such a transfer;
(ii) if the transfer is necessary for the performance of a contract;
(iii) if the transfer is for the benefit of the data subject and it is not practicable to obtain the consent of the data subject for that transfer**.**

Australia

The Privacy Act, 1988 of Australia provides that where an entity discloses personal information about an individual to an overseas recipient, then the Australian Privacy Principles will apply. An entity could mean an agency or an organisation (it is another term for data controller). Australian Privacy Principle 8 applies to the cross-border disclosure of personal information. This principle provides that before an APP entity discloses personal information about an individual to a person (the overseas recipient), who is not located in Australia or if it discloses to someone who is not the data subject, then the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles.

As an exception to this, APP entities are permitted to disclose personal information to the overseas recipient if:

(i) the entity reasonably believes that the recipient is subject to a law, or binding scheme which has the overall effect of protecting the information in a way which is substantially similar to the way in which the APPs protect the information; and
(ii) that there are mechanisms in place which allow the individual to take action to enforce the law or that binding scheme. Additionally, an entity is allowed to disclose personal information to an overseas recipient if she consents to such disclosure, or

if such disclosure is pursuant to an order of a court. Disclosure to overseas recipients is also allowed if the entity reasonably believes that the disclosure of the information is reasonably necessary for the enforcement related activities conducted by an enforcement body.

Canada

Canada's federal privacy laws (PIPEDA) do not prohibit the outsourcing of personal information to another jurisdiction, whether by the private sector or a federal institution. The law in Canada does not distinguish between cross-border and domestic transfers to third parties. They apply the same rules to all third parties, regardless of their location. Third parties include affiliates, subsidiaries and parent organizations. In brief, these laws require organizations to remain accountable for protecting personal information transferred to third parties. This means, in the case of Canada, organizations that hold personal information and transfer it to third parties must include a privacy protection clause in contracts to guarantee that the third party provides the same level of protection as does the organization that originally collected the personal information. In Japan, organizations must establish contracts with service providers and other third parties that contain specific data security provisions.

Two Canadian provinces, British Columbia and Nova Scotia, have enacted laws requiring that personal information held by public institutions—schools, universities, hospitals, government-owned utilities, and public agencies—be stored and accessed only in Canada unless one of a few limited exceptions applies.[24] Canada follows an organization-to-organization approach while dealing with the cross-border transfer of information. Under the PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement or contract. The Canadian Privacy Commissioner investigates complaints and investigates the personal information handling practices of organisations. Principle 1 Schedule 1 of PIPEDA addresses the balance between the protection of personal information of individuals and the business necessity of transferring personal information for various reasons, including the availability of service providers, efficiency and economy. It places responsibility on an organization for protecting personal information under its control.

[24] Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, s. 30.1 (Can.), available at http://www.bclaws.ca/Recon/document/ID/freeside/96165_00; Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, s. 5(1) (Can.), available at http://www.canlii.org/en/ns/laws/stat/ sns-2006-c-3/latest/sns-2006-c-3.html (last accessed on 28.06.2018)

Schedule 1 also provides that personal information may be transferred to third parties for processing, and requires organisations to use contractual or other means to "provide a comparable level of protection while the information is being processed by the third party."

The advantages and disadvantages of a consent-based approach to cross-border data transfers can be summarized as follows:[25]

Advantages

The application of consent, particularly opt-in consent, is the most simple and direct and, in some cases, the least risky means of cross-border data transfers of information as the parties sending and receiving the data assume only the obligations which forms the ground the consent. Also, the mode and the type of consent in most cases can be relatively consistent across all countries. There's no liability on the receiving entity to take on information processing practices. Consent does not necessitate the receiving party to audit information by the concerned authorities of the exporting country. Consent is required in many instances to satisfy local compliance obligations. In Argentina, the EU Member States, Korea, Mauritius, Tunisia and the U.A.E., for example, any processing of "sensitive" data (i.e., specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex[26] life of the individual) usually requires consent. Also, in certain countries there are additional categories of sensitive information such as performance appraisals, criminal background checks and credit checks. Thus, adding a consent to transfer the data across borders can be relatively easy.

Disadvantages

Obtaining consent from all entities (customers, employees, independent contractors and employees of vendors) can be prove be a tedious and costly affair. Several EU DPAs and in particular the Working Party have expressed doubted the validity of consent and the criteria determining a valid consent. Moreover, while this provides a freedom of choice to the parties involved in the transfer, it may also lead to inefficiency, given the party can repudiate or

[25] MIRIAM WUGMEISTER,KARIN RETZER, CYNTHIA RICH, MORRISON & FOERSTER LLP, 'GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES' , available at http://media.mofo.com/docs/pdf/0801CrossBorder.PDF (last accessed on 28.06.2018)
[26] *Ibid*

withdraw their consent at any point without facing any penalties. For ex, an organization in under the EU wants to transfer personal information to a country that has a data protection regime which is not considered "adequate" by the EU, such an information may be discouraged from being transferred, which may ultimately discourage some individuals from providing consent

Criticisms

- **Barriers to Data Flows Undermine Firm Competitiveness and Economic Productivity**

At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries. Such barriers also prevent companies from transferring data that's needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services. Likewise, companies may be compelled to spend more on compliance activities, such as hiring a data-protection officer, or putting in place software and systems to get individuals' or the government's approval to transfer data. These additional costs are either borne by the customer or the firm, which undermines the firm's competitiveness (especially for foreign firms who are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins.

- **Barriers to Cross-Border Data Flows Undermine Innovation and Access to Innovative Services**

Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches. Countries that enact barriers to data flows make it harder and more expensive for their companies to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative new goods and services that rely on data.

CONCLUSIONS AND RECOMMENDATIONS

This paper proposes certain recommendations key to the data privacy movement and what role can these entities play in the same regard.

1. Government of India

The rules under the amended IT act, which is under progress, should set guiding principles for privacy in line with the globally recognized privacy principles. Include all government agencies which collect, process, store, transfer, disclose and use personal information of the end users in the definition of the "Body Corporate"[27]. Channelize sufficient resources and investment on technology research, for promoting academic projects, and creating an infrastructure for this cause. Also, the users should be made aware of the following cause and the threats and the remedies available to them.[28]

2. Law enforcement bodies

They should update themselves with latest trends, technology changes, transactions, user relations etc Develop skills to deal with technology matters that impact the end users under cyber security concepts and how cyber-crimes are committed

3. Industries/ Private Entities

Industries should understand specific privacy needs of their respective industry by dedicating significant efforts on how the industry in general practices and use of technology affects privacy of the end users. They should also have appropriate mechanisms for grievance redressal for the user satisfaction. If an individual gets a set of rights under this policy initiative, it also puts a duty upon an individual to endure his own privacy by taking adequate steps. For ex, having an efficient antivirus software when communication any personal information like in case of banking transactions is a very rudimentary step that can be undertaken. For the success of policy initiatives that can create an impact, both private and government entities, need to

[27] Section 43, Information Technology Act 2000
[28] Policy Paper: Privacy in India, May 2010, 'Data security council of India' available at https://www.dsci.in/sites/default/files/Position-Papers-5-Policy_Paper_Privacy_in_India.pdf (last accessed on 28.06.2018)

work in harmony. Each of these entities, in their respective capacity, can bring the necessary change that promotes a culture of privacy in India.