

REGULATING TRANSBORDER FLOW OF PERSONAL INFORMATION FOR DEVELOPMENT IN THE G77+CHINA GROUP

Lukman Adebisi Abdulrauf

Centre for Human Rights

Faculty of Law

University of Pretoria

Department of Public Law

And University of Ilorin, Nigeria

lukmanrauf@gmail.com

ABSTRACT

Transborder data flow (TBDF) has generated much controversy in this era of globalisation. Various questions regarding its exact nature, dimension and role have been raised by scholars. Nevertheless, the majority of scholars agree that TBDF is crucial for development in every state and even more important for developing countries. In spite of the general consensus that TBDF is vital for development, it raises some concerns such as the infringement of individuals' right to privacy. This has made countries and international organisations regulate TBDF in data protection instruments. Such instruments in some cases put stringent conditions on TBDF, which could be an obstacle to the free movement of personal data across borders and may even serve as a non-tariff barrier against developing countries, including G77 states. The implication of this trend of events is that if G77 states do not take data protection and regulation of TBDF seriously, they may never benefit economically from developed countries. This will, of course, not sit well with the primary purpose for the establishment of the G77+China. With a special focus on the G77, this article examines the role of regulating TBDF in facilitating TBDF for economic development. This topic is

UNISA 
university
of south africa

Latin American Report
Volume 31 | Issue 1 | 2015
pp. 77–96

Print ISSN 0256-6060

crucial in the wake of various initiatives by the G77 to promote trade so as to foster development.

Keywords: trans-border data flow; data protection; personal data; G77; development; regulation

INTRODUCTION

Transborder data flow has become increasingly critical in economic, political and social terms since the adoption of the Organization of Economic Cooperation and Development (OECD) Guidelines on the protection of privacy and transborder flows of personal data in 1980 (OECD Guidelines) (Kuner 2011: 3). With increased globalisation of the world economy, there is greater need for personal data across the world as it has, in recent times, become a very powerful but scary item (Lagos 2014: 187). The greater need for personal data is as a result of the realisation of its significance by both private and public entities.¹ To depict the value of personal data in this globalised digital world, it has been described using several weighty phrases. It is termed a 'crucial raw material' (Kuner 2013: 1), a 'valuable commodity' (Kuvana 2009; Bygrave 2002: 99), and the lifeblood or basic currency of the information economy (Robinson et al. 2009: 12). In fact, it is said that personal data is the new oil of the internet and the new currency of the digital world (Kuvana 2009: 7). It is the hottest commodity on the market today and even more valuable than gold (Craig and Ludloff 2011: 7). Advances in technology and the internet have led to the globalisation of personal information and facilitated its transfers (Kong 2010: 21:1; Bennett and Raab 2003: 257). To enhance development in every modern society therefore, TBDF is imperative. This is even more so for developing countries who must utilise every opportunity at their disposal to maximise resources obtainable from their developed counterpart.

Developing countries have always sought a platform to harmonise their individual efforts towards achieving development. Such a platform came with the establishment of G77, which enables them work in unity to achieve economic growth and development. Thus the G77 gives them a united voice in negotiations on the terms of international trade that will facilitate growth. One means by which these countries can foster development is through TBDF, which is about the free movement of information across borders. TBDF has become a dominant topic in debates on international trade and its importance has been considered by several commentators (Kuner 2011; Mhlaba 1995: 356–366). Its importance is that it brings about economic progress and creates a platform for exchange of resources among nations. This is imperative for developing countries of the G77. In spite of these widely acknowledged benefits of TBDF, there are several challenges associated with it. The most common is the threat to the privacy and security of personal data. This has made many countries, especially developed ones, put in place legal instruments

regulating TBDF. Some of these developed countries have even been said to regulate TBDF for economic protectionist purposes. This therefore means that G77 states must individually and collectively take issues of regulation of TBDF seriously by putting in place the appropriate legal mechanisms. This article is inspired by the fact that issues regarding how TBDF impacts on international trade and economic development is yet to be a focus of law or policy in many countries, especially the G77 (Meltzer 2013: 13).

There is a number of scholarly works on regulating TBDF with respect to international institutions such as the Organization for Economic Cooperation and Development (OECD), the Council of Europe (CoE) and the European Union (EU). Among them are works by Kuner (2013; 2011) and Bygrave (2014). There is, however, no specific literature on regulating TBDF for development in the G77. The absence of scholarly works also shows that TBDF as a topic has scarcely been considered by the G77 as a means to harness resources from their developed counterparts.

Against this background, this article examines the significance of regulating TBDF for development in the G77 states. In so doing, the article is divided into six sections. Section 2 unpacks the concepts of ‘TBDF’, ‘data protection’ and ‘personal data’ within the context of this article. Here, the ambit and scope of the concepts are briefly examined. Section 3 gives a brief historical account of the G77 and its initiatives on TBDF. This is done for the purpose of establishing how crucial TBDF is for the development of the G77 states. In spite of importance of TBDF in the development of countries, Section 4 analyses why it needs to be regulated, thereby restricting its flow. Furthermore, it examines broadly the regulatory framework for TBDF with special focus on regimes that may affect TBDF of and between G77 states. Section 5 examines the role of data protection law in TBDF for development of G77 states. Section 6 reflects on how to enhance TBDF for development in the G77 states.

UNPACKING THE CONCEPTS OF TBDF, DATA PROTECTION, PERSONAL DATA

TBDF is a widely used term (Brown 1984: 2). According to Knoppers, TBDF ‘represents the flow of information with economic and/or cultural value’ (1984:1). This definition shows that the term refers to the flow of all kinds of information generally. Indeed, Novotny acknowledges the fact that data/information in TBDF could be operational, financial, personally identifiable (personal data) and scientific/technical in nature (1981: 110–112). Similarly, Brown, relying on Fishman, contends that the term refers to ‘the electronic transmission of personal and non-personal information across political boundaries for processing and storage in computer files’ (Brown 1984: 2). Within the context of this paper, however, only a category of information – personal data/information – is the focus.² Thus, ‘[t]ransborder flows of personal data’ is a concept that was first adopted by the OECD Guidelines in 1980,

and since then, it has become widely used. The OECD Guidelines define it (TBDF) as the ‘movement of personal data across national borders’ (OECD Article 1; Kuner 2011: 3). The Council of Europe Convention (CoE Convention) adopts the term ‘Transborder flows of personal data’ and it is defined as ‘the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed’ (CoE Convention, Article 12). More recent TBDF regulatory instruments do not give any definition. For example, the European Union Directive (EU Directive) uses the term ‘transfer to a third country of personal data’ without giving any specific definition (Article 25; Kuner 2011: 11). Unfortunately, the 2012 Proposed EU Regulation (EU Regulation) also adopts a similar approach as the EU Directive (EU Regulation, Article 40). In a rather confusing manner, the Asia Pacific Economic Cooperation (APEC) Privacy Framework uses a wide range of terms for TBDF. It uses the terms ‘Information transfer’, ‘information flow across borders’, ‘cross-border information flow’ and ‘cross-border data flow’ to refer to movement of personal data across national borders (Kuner 2011: 11). The majority of these instruments therefore, seem to portray TBDF as movement of personal data from one jurisdiction to others. These definitions, however, present TBDF in a rather simplistic way as they create an impression that TBDF is ‘a discrete act, such as someone pushing a button and causing data to be transferred’ (Kuner 2011: 11). Birnhack argues that TBDF is more complicated than merely describing information in such circumstance as merely ‘flowing’ (2008: 517). He contends that ‘Describing data as “flowing”, as if it were a physical object, does not reflect the global digital environment, in which data is everywhere’ (Birnhack 2008: 517).

Because of the threats associated with TBDF as a result of cross-boundary movements of personal information, it is increasingly regulated in a *sui generis* legislation called data protection law. Data protection is becoming a complex concept, like privacy. Hence, summarising it in a few lines is a difficult task (De Hert and Gutwirth 2009: 3). Nevertheless, it is important to attempt a workable definition so as to show its relationship with the concept of TBDF. De Hert and Gutwirth point out that data protection is a catch-all term for a series of ideas regarding the processing of personal data that governments apply to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance (2009: 3). This definition shows that enhancing TBDF and protecting privacy are conflicting values which data protection law seeks to balance. It does not, however, show the nature of the kind of risk individuals are exposed to.

In a more apt manner, Roos defines data protection as ‘a set of measures aimed at safeguarding individuals (data subjects) from harm, resulting from the computerised or manual processing of their personal information by data controllers’ (2008: 313). These measures comprise a group of principles on the processing of personal information (Roos 2008: 313). Two important phrases common in these definitions are ‘processing’ and ‘personal data/information’. These terms are at the very heart of

data protection law. Processing means any operation, activity, or set of operations, which is performed on personal data, whether manually or automatically and such operation or activity includes collection, storage, updating, dissemination, erasure, destruction or transfer (POPIA, sec 1; EU Directive: Art 2(b)). The word processing covers a wide range of activities on personal data, which makes Kuner observe that ‘it is difficult to conceive of any operation performed on personal data in electronic commerce which would not be covered by it’ (Kuner 2007: 74). Thus, TBDF, which basically involves the dissemination or transfer of personal information across borders, is also a processing activity within the context of data protection law.

The regulation of TBDF for the purpose of privacy and data protection does not cover all kinds of data. Data protection law focuses only on personal data narrowly construed as ‘any information relating to an identified or identifiable natural person’ (EU Directive: Article 2). This implies any data that relates to an identified or identifiable individuals.³ Processing of this category, personal data, presents certain risk, which is why a dedicated legal structure (data protection) is put in place for its protection. Processing of certain categories of personal data may, however, not fall within the ambit of data protection law. Such categories include personal information processed in the course of personal activity,⁴ de-identified data,⁵ information collected for public interest, and information processed for journalistic and artistic purposes (POPIA: Section 4).

G77 AND TRANS-BORDER DATA FLOWS

A brief historical account is important for a proper contextualisation of the purpose and objective of the G77. Established in 1964, G77, as the name implies, is a group of seventy-seven developing countries that signed the Joint Declaration of the seventy-seven developing countries.⁶ The Declaration was issued at the end of the first session of the United Nation Conference on Trade and Development (UNCTAD) in Geneva.⁷ The UNCTAD is a United Nation (UN) body responsible for development issues with particular focus on international trade.⁸ A permanent institutional structure for the G77 was established with the first Ministerial Meeting of the Group in Algiers, which adopted the Charter of Algiers.⁹ The G77 has subsequently increased to 134 members, making it the largest intergovernmental organisation of developing countries in the UN, though the original name was retained due to its historical significance.¹⁰ The historical relationship of G77 with UNCTAD goes to show that the former is primarily established to facilitate economic growth of developing countries through international trade. Thus a group of this nature will boost the negotiating capacity of developing economies in major international economic issues and promote co-operation for development.¹¹ Several means are used by the G77 to achieve the realisation of its goal of enhancing economic development in member states. One such means is the avenue it provides in its meetings for the exchange of knowledge, ideas and information (including personal data) between

member states and developed countries. Thus, information must be able to flow freely across borders.

Legal framework for TBDF in the G77

With regard to TBDF, none of the G77 foundation documents contain provisions on the transfer of personal data across borders.¹² Nevertheless, the G77 legal instruments make elaborate provisions for transfer of technology, knowledge and patents between developing and developed countries. This may also indirectly affect TBDF. For example, Part E paragraph 7 of the Charter of Algiers provides that:

- a. The developed countries should encourage the transfer of knowledge and technology to developing countries by permitting the use of industrial patents on the best possible terms, which will enable products manufactured in developing countries to compete effectively in world markets;
- b. They should also promote the elimination of restrictive practices, relating to market distribution and price-fixing, which are imposed by enterprises in developed countries in granting licences for the use of patents and trade-marks in developing countries;
- c. The developed countries should provide guidance to their industrial entrepreneurs regarding investment opportunities in the export industries of the developing countries and familiarise them with legal, political, economic and other relevant information on the situation in the developing countries.

In this regard, it has been argued that technology and knowledge transfer raises issues of TBDF. For example, Knoppers contends that ‘Transborder data flow and technology transfer issues have a substantial overlap’ (1984: 1). According to Knoppers, TBDF issues are the key form of technology transfer.¹³ As information technology plays an increasingly important role in areas such as engineering and research, ‘an increasing portion of our “know-how” and accompanying information is created, processed, stored, and disseminated in electronic or digitalized form (only)’ (Knoppers 1984:1). It is therefore submitted that the accompanying information being referred to includes personal information. From this premise, it is arguable that knowledge and technology transfer will also involve movement of personal information across borders. The World Economic Forum observed with regard to the importance of personal information in knowledge transfer that:

To stay current, stakeholders should share insights and learnings on their relevant activities, from both successes as well as failures. After all, the ecosystem’s promise is about the tremendous value created when individuals share information about who they are and what they know (WEF 2011: 12).

Therefore, although remote, the relevant provisions of the above quoted provision of the Charter of Algiers may be construed also to mean encouraging the transfer

of personal data since it is also a resource that developing countries (G77 states)¹⁴ will need. There are also numerous provisions on trade liberalisation, especially with regard to the removal of trade barriers to free movement of goods and services between developed and developing states (Charter of Algiers: part 2, para 2). Since scholars have generally contended that personal information is now a commodity or a resources, then it is arguable that ‘goods’ within the context of trade liberalisation also include personal information. Indeed, Sauvart contends that discussions on TBDF ‘increasingly recognize that data flows are commodity flows (either in their own right or because they are closely related to trade flows in other areas, such as shipping) and that, therefore, the subject matter should be regarded as an economic issue’ (1983: 360). It goes without saying also that service trade between developed and developing countries will also involve TBDF. For example, an agreement on provision of professional services by engineers or construction workers between Nigeria and Germany will involve movement of personal information between the contracting parties.

Issues of TBDF are also rarely considered in Ministerial declarations in spite of the encouragement of global partnership for development among states. This is surprising as developing countries have been urged to take account of ‘changing context’ in the transfer of technology (UNCTAD: 5). Indeed, the reference to a ‘changing context’ in the transfer of technology should, arguably, involve the increasing prominence of TBDF in such transfers. Some Ministerial declarations, however, encourage initiatives on issues related to TBDF, such as technology transfer and information sharing on science and technology among states. As noted above, this will arguably include TBDF. The above shows that none of the documents have considered the significance of TBDF as a means of fostering development.

The importance of TBDF for development of G77 states

With globalisation and the so-called ‘information revolution’, TBDF becomes very significant for developing countries. Unfortunately, little empirical research has been done to evaluate the impact of TBDF to depict its significance (Kuner 2013:5; Mutai 2013: 8). Nevertheless, it has aptly been noted that ‘[t]he ability to transfer personal data internationally is assuming ever-increasing importance in promoting economic and social development’ (Kuner 2011: 8). Thus, ‘[t]he international transfer of increasing amounts of personal data and the growth of electronic commerce have resulted in economic growth and efficiencies that have had a positive impact around the world’ (Kuner 2011: 10). According to the OECD, the growth of the internet together with the ability to move data rapidly is a key building block of the global economic order (Kuner 2013: 5; Meltzer 2013: 4). G77 states will, no doubt, benefit from the growing economic importance of cross-border data flows in the past few years, which has created new markets and unlocked numerous economic resources.

Unfortunately, there is a general absence of qualitative data on TBDF to evaluate its practical significance, especially to developing countries of the G77 (Mutai 2013: 5).

Different countries are endowed with different economic resources. From this perspective, there is a need for countries to exchange resources so as to reap the benefits of economies of scales, division of labour and specialisation. Outsourcing transactions presents such an opportunity for developing countries of the G77 with the aid of TBDF. According to Greaver, '[o]utsourcing is the act of transferring some of an organization's recurring internal activities and decision rights to outsider providers [usually offshore], as set forth in a contract' (1999: 3). This process naturally involves movement of personal information. For example, during the due diligence and negotiation stages of an outsourcing contract, personal information of employees, customers and directors will be transferred between the contracting parties. Some of the potential benefits of outsourcing, according to McIvor, include cost reduction, performance improvements, flexibility, specialisation and access to innovation (2005: 21–23). Outsourced tasks are usually less effective and more expensive if they were to be carried out 'in house' (Stefanick 2007: 532). G77 member countries therefore stand a chance to benefit from outsourcing contracts propelled by TBDF as businesses could focus on their core functions that could lead to firm growth (Mutai 2013: 9).

Another important role of TBDF, according to Poulet, is the opportunity it creates for the transfer of personal information for the purpose of executing contracts, or for technical purposes such as for the purpose of processing, analysis or storage abroad (2009: 4). In this respect, Mutai observes that companies could enter foreign markets without necessarily having a physical presence there (Mutai 2013: 9). This is even more so because of the comparative cost advantage brought about by the relative advances in cloud computing. Furthermore, a common economic benefit of exporting personal data to a third country is for ease of administration, especially of multinational enterprises (MNEs) (Mutai 2013: 9). It is now common for multinationals to pool the data of all operating divisions and subsidiaries in one common databank with the aid of advances in technology (Knoppers 1984: 1; Sauvant 1983: 361). Thus, MNEs are increasingly dependent on the fast and reliable movements of information across borders (Mutai 2013: 2), so much so that Sauvant contends that TBDF have become the lifeblood of their operations (1983: 361; Kong 2010: 1). In this regard, a number of G77 states are hosts to large companies with headquarters in other parts of the world – mostly in developed countries. For example, multinationals such as Mastercard, Unilever, Accenture, Shell and Chevron have subsidiaries or affiliates in many African countries. Exporting employees and business data brings about effective administration as a common database is built in different countries, which may help improve productivity. From the point of view of e-commerce, which is supported by TBDF, developing countries and consumers in these countries stand to benefit. Indeed, the importance of e-commerce to developing countries cannot be overemphasised (Ray 2011). According to Ray, e-commerce

(technologies) helps developed countries access markets of developing countries (2011: 7). TBDF, supported by the internet and e-commerce, has benefits to consumers within G77 states. For example, Meltzer argues that TBDF has revolutionised the finance industry in that consumers can now access their accounts and accountants globally (2013: 4). Similarly, business in developing countries can access market-leading financial services in countries such as the US and UK (Meltzer 2013:4). Meltzer also observes that large companies in developed countries are also taking advantage of the opportunities TBDF creates to increase access to capital start-ups (2013: 4). For example, 33needs, a web application business, connects investors with small-scale entrepreneurs in developing countries (Meltzer 2013: 4).

The above shows the significance of TBDF for developing countries. The G-77 states may, however, not be able to benefit from the TBDF transactions because of the growing trend in regulation of data transfers by the developed countries. The reasons for these regulations will now be considered.

From the foregoing, TBDF is beneficial to G77 states, especially from economic and commercial perspectives. Nevertheless, south-south cooperation may be significantly hampered by the increasing regulation of TBDF, especially by developed countries. The following section discusses why states (developed countries) regulate TBDF and the major international instruments that have the effect of restricting TBDF.

WHY DO STATES REGULATE TBDF?

A number of reasons led to the regulation of TBDF. Knoppers identifies economic and sovereign concerns as the main reasons why states increasingly regulate TBDF (1984: 3–11). Economic concern, by and large, is for the purpose of protecting trade and balance of payment of a country that could be jeopardized if large amounts of data of a country are processed in another country (Knoppers 1984: 3). Sovereignty concerns, on the other hand, include national security, legal issues and cultural impacts (Knoppers 1984: 4). With specific reference to cross-border transfer of personal information, Kuner identifies four reasons why states regulate TBDF (2011: 7, 23, 24). Firstly is to prevent the circumvention of national data protection laws by transferring personal information to so-called ‘data havens’. In this regard, a TBDF regulation of a country prevents businesses from transferring personal information to third countries without TBDF regulations for processing so as to circumvent the laws in their home country, that is, data havens. The processing of personal data brings about reasonable incentives for business to do all that is necessary to circumvent the law. For example, Section 4b of the Federal Data Protection Act of Germany 2003 provides that transfer to a foreign country outside Germany (or the EU) can only be effected if the third country has an adequate data protection regime. This section effectively bars data processors from transferring information to a third country without an effective data protection regime so as to circumvent the Act.

Secondly, regulating TBDF will help protect individuals from the risks (privacy and data protection) they may be exposed to if their personal data is processed in other countries. A third reason is to address the difficulties in claiming data protection rights abroad. Because of issues of sovereignty, individuals and regulators may not be able to move against infringements of their privacy related rights abroad. However, with rules on TBDF, there is increased cooperation between regulatory authorities in various jurisdictions, which makes enforcement of privacy related rights easier. Lastly, TBDF is regulated so as to enhance consumer and individual confidence (Kuner 2011: 7; Donohue 2015: 20).

Of the above-mentioned reasons, the second arguably is the most common justification by states for regulating TBDF (Meltzer 2013: 6). Engaging in TBDF without appropriate regulations could bring about certain risks to both individuals of the developed country and the G77 state. Such risks are largely human rights related, such as violation of individuals' right to privacy. Indeed, a commentator observes that '[t]o date, privacy concerns have dominated the TBDF debate at the international level' (Knoppers 1984: 3). Violation of individuals' privacy may also occur if individuals' personal data falls into the wrong hands in the receiving state, which may in turn cause identity thefts and expose individuals to cybercriminals. Roos considers other possible risks to data processing, which also applies to TBDF. She states that personal data being transferred may be inaccurate, incomplete or irrelevant, accessed or disclosed without authorisation, and used for a purpose other than that for which they were collected or unlawfully destroyed (Roos 2008: 314). TBDF raises issues such as if an entity in the receiving state will put in place equivalent (or adequate) mechanisms to ensure its personal data is properly safeguarded. All these threats will naturally make consumers wary of engaging in e-commerce, except if an appropriate framework is in place to make them confident in the system.

There are two other important reasons why states regulate TBDF, which were not contained in Kuner's discussion (2011: 7). Firstly is the economic benefit accruing to G77 state by such regulation. In this regard, Mutai argues that regulation of TBDF may bring economic benefits to a country as other countries will be more willing to transfer personal data to such a country. Secondly, it has been argued that government regulates (restricts) TBDF for less legitimate and controversial reasons, such as to cause commercial loss to foreign business while promoting local companies (Meltzer 2013: 5).

The increasing threats TBDF places on personal data has made various legal systems regulate its free flow. It must, however, be pointed out that the primary objective of these normative frameworks is not to totally prohibit the flow of personal data (De Hert and Gutwirth 2009: 3). Rather, these instruments establish structures to enhance transfer while also protecting the privacy interests of individuals' subject of the information.

REGULATORY FRAMEWORK FOR TBDF IN INTERNATIONAL LAW

The first set of responses to challenges of data privacy resulting from TBDF were within domestic laws of certain European countries such as Sweden and Germany (Lloyd 2011: 22). The expansion in TBDF across jurisdictions led to initiatives for its regulation by various international organisations, starting with the OECD. Today, more than 70 countries, including some G77 states, have enacted laws with provisions regulating TBDF (Kuner 2011: 6).¹⁵ Many of these countries are developed countries, especially in Europe. Similarly, many international organisations have instruments regulating TBDF. This section focuses on the international or regional instruments on TBDF. Some of these international instruments do not directly affect most G77 states because they are not state parties to them. Nevertheless, these instruments may indirectly affect transfer of personal information between a developed country and a G77 state, and this may be an obstacle to realise the objectives of the G77. Thus, it is imperative to consider briefly these instruments.

It must be pointed out that there are two major approaches to regulating TBDF to protect personal data. While some types are geographically based, others make data exporters accountable for the continued protection of individuals' personal data transferred irrespective of the geographical location (Kuner 2011: 7). In this regard, the EU and most of its members adopt the first approach while the APEC and some of its member economies adopt the second approach.

Because of the widely acknowledged benefits of TBDF to the development of countries, many of the legal instruments are, as a general rule, drafted in a way that encourages free flow of personal data across borders. Restricting trans-border data transfer is only an exception to the general rule and subject to some conditions.

As earlier stated, the OECD Guidelines was the first document to provide for TBDF. Part 3 of the guidelines generally provides for 'basic principles of international application: free flow and legitimate restrictions'. Article 16 requires member countries to take all reasonable and appropriate steps to ensure that TBDF including transit through member country are uninterrupted and secure (OECD Guidelines). A member country is also required to refrain from restricting flow of personal data except where another member country has not substantially observed the Guidelines, or where re-export of such data would circumvent its domestic privacy legislation (OECD Guidelines, paragraph 17). Member countries should also not establish laws and policies in the name of privacy which will obstruct TBDF that will exceed requirements for such protection (OECD Guidelines: paragraph 18). Based on this provision, it is clear that the OECD Guidelines only regulate TBDF between member countries. This may have little effect on TBDF for G77 states as none of the G77 states are members of the OECD.¹⁶

The Council of Europe Convention is also applicable to member states only. Recent amendment of the Convention has, however, made it possible for non-

European member states to be parties to the treaty.¹⁷ Chapter 3 of the Convention regulates TBDF. The Convention prohibits any obstacle to TBDF. It provides that ‘a party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another party’. Some conditions for derogations are provided. This provision also applies to TBDF within states parties which include some G77 states.¹⁸ Nevertheless, an Additional Protocol to the Convention will make it applicable to all G77 states. Article 2(1) of the Additional Protocol provides that:

Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer (CoE Additional Protocol: Article 12(1)).

The above provision also requires adequate level of protection by a G77 state not being state parties to the OECD. The UN Guideline principles also provide in Article 9 that personal data ‘should be able to circulate freely’ provided the legislation of the countries concerned ‘offer comparable safeguards for the protection of privacy’ (CoE Additional Protocol: Article 9). It is further provided that ‘if there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands’ (CoE Additional Protocol: Article 9).

The most influential and aggressive regulatory framework for TBDF is the EU Directive. The Directive is described by a commentator as ‘the leading force of globalizing data protection’ (Birnhack 2008: 512). The Directive, according to Mantelero, was ‘inspired not only by the intention of removing obstacles to flows of personal data in order to facilitate economic activities, but also by the aim of offering a high level of protection of individual rights’ (2012: 3). This instrument, though applicable to EU member states only, has an extra-territorial effect that impacts on G77 states. Article 25 of the Directive provides that personal information from an EU member state can only be transferred to a non-member state that has an adequate data protection regime (EU Directive, Art 25). The Directive also specifies a special mechanism for determining adequacy (EU Directive, Article 25(6)). In addition, some exceptions are provided from the general rule that permits extra-territorial transfer of data (EU Directive, Article 26; Birnhack 2008, 24: 513)). Based on the EU approach in the Directive, any G77 state desirous of having a business dealing with an European country must have a TBDF regime that is deemed ‘adequate’ by the EU.¹⁹ The EU’s approach to regulation of TBDF has drawn criticisms for a commentator who argues that Europe is trying to impose its data protection regime on the world (Makulilo 2013: 447). This is because it is contended that:

The indirect effect of this rule [article 25] is to induce the countries interested in having commercial relations with the EU to adopt similar data protection laws. In the absence of these laws, local companies are not be able to work with European partners, because they cannot receive personal data concerning consumers, suppliers and partners (Mantelero 2013: 3).

Birnhack rejects this contention and argues that Europe cannot be said to impose its regime on the world because the directive is a non-binding international treaty. According to him, the Directive rather ‘applies a sophisticated, inducing mechanism to spread its gospel’ (Birnhack 2008: 512). The EU directive is the greatest obstacle to TBDF of G77 states especially with Europe. This is because no data protection law of any G77 state has been declared adequate by the EU Commission. What this means is that a non-European country (G77 state) cannot freely receive personal information from any European country based on the general requirements of Article 25. For example, a company in a G77 country that offers certain services such as advertising, which may require collection of personal information from the EU, will be restricted from engaging in such transaction by Article 25. G77 member states may, however, resort to the exception provides in Article 26 of the directive, which may be a more cumbersome and bureaucratic process.

Rather than the forceful approach of the EU directive in regulating TBDF, the APEC Privacy Framework adopts a milder approach. It provides that personal data should be processed in a way that protects individuals’ information privacy and allows them to realise the benefits of information flows within and across borders (APEC Privacy Framework, paragraph 29). Protection of personal data in the course of TBDF is realised under the APEC Privacy Framework through the accountability principle (APEC Privacy Framework, paragraph 26). The framework holds a transferor accountable for complying with measures to give effect to all the other principles (APEC Privacy Framework, para 26). This provision is applicable to data processing generally. Quite a number of developed countries belong to the APEC and are bound by the Privacy Framework. A transferor from an APEC member economy like Canada will have an additional burden, which may hamper TBDF to a developing G77 country.

THE ROLE OF DATA PROTECTION LEGAL INSTRUMENTS IN TBDF FOR DEVELOPMENT IN G77 STATES

TBDF is crucial for economic growth and development of the G77 states. TBDF is usually regulated within the data protection legal instrument. Thus, to enhance TBDF, data protection law is imperative for three major reasons. First, it brings about economic benefits to G77 states. Second, the data protection legal framework will facilitate access to vibrant information market in jurisdictions or regions with strict requirements on transfer of personal data. Third, it will enhance consumer confidence in the system, which will enable them to participate more in e-commerce (Kuner 2013: 2).

It is generally known that the economic benefits of data protection legal instrument regulating TBDF are significant. The most important benefit is that it

creates an opportunity to trade with developed countries. Many countries will freely allow transfers of personal data when they are guaranteed of equivalent protection in the receiving country (Kuner 2011: 24).²⁰ This will create economic benefits for the receiving states, in this case, the G77 states (Kuner 2011: 24). It will create an opportunity for outsourcing deals and serve as an incentive for MNEs to further invest in developing countries. This has a multiplier effect of job creation and economic and infrastructural improvement in a developing G77 country.

With respect to enhancing access to information market, the EU jurisdiction makes this issue significant. The EU has been stated to be the largest trading bloc in the world, which means no country or group can afford to ignore its rules.²¹ To enable access to the EU information and commodity market, G77 states, either individually or collectively, need to have a legal framework considered 'adequate' by the EU based on the requirement of the EU Directive. Another dimension of the significance of data protection law for TBDF goes to the very basis for which the G77 was established. Developed countries within EU can only assist developing countries, especially with respect to transfer of science and technology when the latter possess adequate regulations on TBDF. This is because in most cases, transfer of science and technology may include personal data of European citizens. Transfer of personal data out of Europe cannot otherwise be carried out in the absence of the TBDF regulatory framework in the receiving state. Moreover, the EU Directive makes it a mandatory requirement that member states 'shall take the measures necessary' to prevent any data transfer to states without an adequate data protection regime (EU Directive, Art 25(6)).

The provision restricting data transfers to jurisdictions without 'adequate' data protection instrument has been argued to serve economic protectionist purposes (Caruana and Cannataci 2007: 105). It is that contended this may effectively serve as a non-tariff barrier in favour of European states. Without prejudice to the truthfulness (or otherwise) of this assertion, G77 states can only circumvent this barrier when they have in place legal instruments on data protection. The EU will therefore have no reason to prevent data transfers to G77 member states under the guide of a lack of data protection instruments.

Availability of adequate data protection instruments in G77 states will enhance individuals' confidence in TBDF system. This will make them participate more in transactions that involve TBDF. After all, Kuner has stated that with advances in technology, TBDF has grown to mean more than big business engaging in transfers of personal data (2011: 3). An individual may also need to access certain services or carry out some transaction across borders using the internet. This will boost e-commerce and therefore bring about development in G77 states.

The G77 leaders in a recent declaration have acknowledged the importance of protection of privacy, although not on the grounds of promotion of TBDF. The leaders were concerned about the use of ICTs to violate human rights and fundamental freedoms especially by developed countries (Khor 2014: 10–15).

CONCLUDING REMARKS

In conclusion, a number of important findings are made with regard to regulating TBDF for development in the G77. First, TBDF, in spite of its immense significance, has not been seriously considered by the G77. Secondly, because TBDF has not been considered, the benefits accruable to member states in regulating TBDF have also not been discussed. Thirdly, quite a number of G77 states, in spite of the significance of regulating TBDF, have no legal instrument regulating TBDF. For example, out of 54 African countries that are all members of the G77, only 14 have legal instruments regulating TBDF (Makulilo 2015:9).

A discussion on regulating TBDF for development in the G77 states is crucial in the wake of the increasing globalisation of the world, which is largely brought about by advances in technology. Given that the free movement of information, goods and services are one of the major features of a globalised world, every community must put in place adequate measure to flow with the tide of globalisation. The G77, which primarily seeks to foster economic growth of developing states, must therefore not be left behind in regulating TBDF for the purpose of data protection.

It is therefore recommended that the G77 should operate as a group for the purpose of regulating TBDF. First, the G77 as a body must have a framework on TBDF (and its regulation) with adequate provisions, like that of advanced countries. This framework must also be followed with a rigorous oversight and implementation mechanism. It is important that the G77 functions as a group because it will facilitate harmonisation and unification of data protection policies. This will create an atmosphere of certainty in the application of data protection law for development purposes. Second, even though a number of G77 states have individually adopted TBDF instruments and enacted data protection laws, a number of them are still lagging behind in this regard, like Nigeria. Similarly, none of the G77 member states with a TBDF regime is yet to be declared 'adequate' by international institutions such as the CoE and the EU. This means that the G77 as a group must put in place a mechanism with a view achieving far-reaching reforms in member states. The group initiative should also be complemented by individual efforts of enacting data protection laws by individual state parties. These suggestions will make developed countries have confidence in the TBDF system of G77 states and open up their markets. This will serve as a double advantage in not only enabling access to the information markets of advanced nations, but will also guarantee human right to data protection of their citizens. Individuals as consumers will therefore be encouraged to participate in e-commerce and TBDF activities.

NOTES

1. Personal data is increasingly needed by private entities for commercial purposes. Many services offered to consumers rely heavily on aggregated data. Retailers need to know more

about their customers so as to be able to market their goods and services through direct marketing. They also need customer personal information for marketing purposes. Public entities such as the government need individuals' personal information for law enforcement and crime prevention, welfare, budgeting. For more on the economic uses of personal information, see WEF (2011).

2. Both terms are used interchangeably in this paper even though a distinction can be drawn between them. According to Roos, data is unstructured or unorganised facts that need to be processed and organised to produce information. Information is thus a set of organised, structured and processed data (2008: 313). Bygrave opines that 'it is artificial and unnecessarily pedantic ... to maintain a division between the two notions, as such a division is usually difficult to maintain in practice' (2002: 20).
3. Some jurisdictions also include data that identifies a legal or corporate person as part of personal data and therefore within the scope of data protection law (POPIA: sec 1).
4. This includes information which, for example, is collected in a personal diary or mobile phone for pure personal purposes.
5. De-identified data means to delete any information that identifies the subject (POPIA: sec 1).
6. G-77, 'About the Group of 77'.
7. Ibid. See Joint declaration of the seventy-seven developing countries made at the conclusion of the United Nations Conference On Trade And Development. Available at <http://www.g77.org/doc/Joint%20Declaration.html> (accessed 10 April 2015).
8. UNCTAD, 'About us. According to the UNCTAD website, it is 'a forum where representatives of all countries can freely engage in dialogue and discuss ways to establish a better balance in the global economy'. It also 'offers direct technical assistance to developing countries and countries with economies in transition, helping them to build the capacities they need to become equitably integrated into the global economy and improve the well-being of their populations'.
9. In 1967. See First Ministerial Meeting of the Group of 77: Charter of Algiers.
10. G-77, 'About the Group of 77'.
11. Ibid.
12. G-77, First Ministerial Meeting of the Group of 77: Charter of Algiers.
13. See, for example, the 2013 declaration that states that The Ministers accordingly underscored the need for a strengthened and scaled-up global partnership for development, based on the recognition of national leadership and ownership of development strategies. They emphasised that international cooperation must be enhanced, including the fulfilment of commitments of internationally agreed official development assistance, debt relief, market access, capacity building and technical support, including technology transfer. See Para 9 of Ministerial Declaration adopted at the thirty-seventh annual meeting of the Ministers for Foreign Affairs of the States Members of the Group of 77, New York 26 September 2013 Available at [http://www.g77.org/doc/A-68-595\(E\).pdf](http://www.g77.org/doc/A-68-595(E).pdf) (accessed 10 April 2015).
14. See Para 9 of Conclusions and recommendations of the meeting of Ministers of Science and Technology of the member States of the Group of 77, Brazil, 3 September 2006. Available at [http://www.g77.org/doc/docs/A-61-382%20\(English\).pdf](http://www.g77.org/doc/docs/A-61-382%20(English).pdf) (accessed 10 April 2015).
15. Argentina, Uruguay, Bahamas, Bosnia and Herzegovina, Benin, Burkina Faso, Mauritius, Morocco, South Africa and Tunisia (Kuner 2011: 6).

16. Members of the OECD include Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom and United states. See OECD, 'List of OECD Member countries- Ratification of the Convention on the OECD'.
17. In 2011, Uruguay became the 1st non-state member followed by Morocco in 2013. See Greenleaf, 'Morocco and Uruguay start Convention 108's Journey to Global privacy Treaty'.
18. For example, Bosnia Herzegovina. See CoE, 'Member states of the Council of Europe'.
19. Kong argues that the approach serves as an external push for third countries to improve their data protection. (2010: 445).
20. Though Kuner was quick to admit that 'little "hard" research has been done to confirm the effects of transborder data flow regulation' (2011: 24).
21. European Commission, 'Trade: EU position in world trade'. It was stated that 'The EU is the world's largest trading block. The EU is the world's largest trader of manufactured goods and services.'

REFERENCES

- Asia Pacific Economic Cooperation (APEC). Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (accessed 10 April 2015).
- Bennett, C. and Raab, C. 2003. *The governance of privacy: Policy instruments in global perspective*. Farnham: Ashgate.
- Birnback, M. 2008. The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Report*, 24: 508–520.
- Brown, R. Wellington. 1984. Economic and trade related aspects of transborder data flow: Elements of a Code for transnational commerce perspectives. *Northwestern Journal of International Law and Business*, 6(1): 1–85.
- Bygrave, Lee A. 2002. *Data protection law: Approaching its rationale, logic and limits*. Netherlands: Springer.
- Council of Europe (CoE). Member states of the Council of Europe. Council of Europe. Available at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG> (accessed 10 April 2015).
- Council of Europe (CoE). 2001. Additional Protocol to the Convention for the Protection of Individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows. Available at <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm> (accessed 10 April 2015).
- Craig, T. and Ludloff, E. Mary. 2011. *Privacy and Big Data*. Sebastopol: O'Reilly Media, Inc.
- Caruana, M. Mireille and Cannataci, Joseph A. 2007. European Union privacy and data protection principles: Compatibility with culture and legal frameworks in Islamic states. *Information & Communications Technology Law*, 16(2): 99–124.

- De Hert, P and Gutwirth, S. 2009. Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in ACTION. In Gutwirth, S., Poullet, Y., De Hert, P., de Terwange, C. and Nouwt, S. (eds.), *Reinventing data protection?* Netherlands: Springer.
- Donohue, K. Laura. 2015. High technology, consumer privacy, and US national security. *Business Law Review*, forthcoming. Available at <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1119&context=cong> (accessed 10 April 2015).
- European Union (EU) Directive. Directive 95/46/EC 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. OJL281, 23/11/1995 P. 0031 – 0050. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (accessed 10 April 2015).
- European Commission. European Commission Proposal for a Regulation Of The European Parliament And of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012). Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 10 April 2015).
- European Commission. Trade: EU position in world trade. Trade. Available at <http://ec.europa.eu/trade/policy/eu-position-in-world-trade/> (accessed 10 April 2015).
- G-77. About the Group of 77. The Group of 77 at the United Nations. Available at <http://www.g77.org/doc/index.html> (accessed 10 April 2015).
- G-77. First Ministerial Meeting of the Group of 77: Charter of Algiers, 1967. <http://www.g77.org/doc/algier~1.htm> (accessed 10 April 2015).
- Greaver, F. Maurice. 1999. *Strategic outsourcing: A structured approach to outsourcing decisions and initiatives*. New York: AMACOM (Div American Mgmt Assn).
- Greenleaf, G. 2013. Morocco and Uruguay start Convention 108's Journey to Global privacy Treaty. *Privacy Laws & Business International Report*, 122: 20–23.
- Khor, M. 2014. G77 declaration addresses 'global challenges'. *Third World Economics*, 572/573: 10–15.
- Knoppers, J.V.T. 1984. Transborder Data Flow Issues and Technology Transfer. *Journal of Technology Transfer*, 9(1): 1–14.
- Kong, L. 2010. Data protection and transborder data flow in the European and global context. *European Journal of International Law*, 21(2): 441–456.
- Kuner, C. 2013. *Transborder data flows and data privacy law*. Oxford: Oxford University Press.
- Kuner, C. 2007. *European data protection law: Corporate compliance and regulation*. Oxford: Oxford University Press.
- Kuvena, M. 2009. Speech delivered at Roundtable on Online Data Collection, Targeting and Profiling. Brussels, 31 March 2009. Available at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (accessed 10 April 2015).
- Lagos, Y. 2014. Taking the personal out of data: Making sense of de-identification. *Indiana Law Review*, 48: 187–203.
- Lloyd, I.J. 2011. *Information technology law*. Oxford: Oxford University Press.
- Makulilo, A. Boniface. 2013. 'One size fits all': Does Europe impose its data protection regime on Africa? *Datenschutz und Datensicherheit*, 7: 447–451.

- Makulilo, A. Boniface. 2015. Privacy in mobile money: Central banks in Africa and their regulator limits. *International Journal of Law and Information technology*: 1–20.
- Mantelero, A. 2012. Cloud computing, trans-border data flows and the European Directive 95/46/EC: Applicable law and task distribution. *European Journal of Law and Technology*, 3(2).
- McIvor, R. 2005. *The outsourcing process: Strategies for evaluation and management*. Cambridge: Cambridge University Press.
- Meltzer, J. 2013. The internet, cross-border data flows and international trade. *Issues in Technology Innovation*, 22: 1–20. Also available at <http://www.brookings.edu/~media/research/files/papers/2013/02/25-international-data-flows-meltzer/internet-data-and-trade-meltzer.pdf> (accessed 10 April 2015).
- Mhlaba, S.L. 1995. The efficacy of international regulation of transborder data flows: The case for the Clipper Chip. *Government Information Quarterly*, 12(4): 353–366.
- Mutai, M. 2013. Trans-border data flow: Its advantage and disadvantages. Available at <https://www.mu.ac.ke/informationsscience/index.php/research-publications/staff-research-and-publication-2/category/16-miriam-mutai?download=57:advantages-and-disadvantages-of-trans-border-dataflow> (accessed 10 April 2015).
- Novotny, J. Eric. 1981. Transborder data flow regulation: Technical issues of legal concern. *The John Marshall Journal of Information Technology and Privacy Law*, 3(1): 105–124.
- Organization for Economic Cooperation and Development (OECD). Guidelines on the protection of privacy and transborder flows of personal data. Organization for Economic Cooperation and Development. 1980. Available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm> (accessed 10 April 2015).
- Organization for Economic Cooperation and Development (OECD). List of OECD Member countries- Ratification of the Convention on the OECD. Available at <http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm> (accessed 10 April 2015).
- Pouillet, Y. 2007. Transborder data flows and extraterritoriality: The European position. Available at http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/pouillet_/pouillet_en.pdf (accessed 10 April 2015).
- Ray, S. Jeffrey. 2011. Leveling e-commerce opportunities for developing countries. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2108365 (accessed 10 April 2015).
- Robinson, N., Graux, H., Botterman, M. and Valeri, L. 2009. Review of the European Data Protection Directive, (Technical report). RAND Corporation. Available at http://www.rand.org/pubs/technical_reports/TR710.html (accessed 10 April 2015).
- Roos, A. 2008. Data protection. In Van Der Merwe, D., Roos, A., Pistorius, T. and Eiselen, S. (eds.), *Information and communications technology law*. Durban: LexisNexis.
- Savant, P. Karl. 1983. Transborder data flows and the developing countries. *International Organization*, 37(2): 359–371.
- South African Protection of Personal Information Act (POPIA) (no. 4 of 2013).
- Stefanick, L. 2007. Outsourcing and transborder data flows: The challenge of protecting personal information under the shadow of the USA Patriot Act. *International Review of Administrative Sciences*, 73(4): 531–548.

The Council of Europe Convention (CoE). The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS no. 108. Available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (accessed 10 April 2015).

United Nations Conference on Trade and Development (UNCTAD). 2001. Transfer of technology. New York and Geneva: United Nations Publications. Available at <http://unctad.org/en/docs/psiteiitd28.en.pdf> (accessed 10 April 2015).

United Nations Conference on Trade and Development (UNCTAD). About us. Available at <http://unctad.org/en/Pages/AboutUs.aspx> (accessed 10 April 2015).

World Economic Forum (WEF). 2011. Personal data: The emergence of a new asset class. Available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 10 April 2015).