Alex B. Makulilo

"One size fits all": Does Europe impose its data protection regime on Africa?

Just before the Directive 95/46/EC on the regulation of processing of personal data in the European Union (EU) and the European Economic Area (EEA) came into force, a debate had ushered that Europe wanted to legislate for the whole world. The debate was and is still dominant among European and American scholars. This article sets to interrogate this debate and more particularly discuss the place of Africa in the debate. The article also assesses the overall impact of the trans-Atlantic debate in the development of data protection laws in Africa.

1 Introduction

As time goes by non-European countries increasingly adopt comprehensive data protection legislation in the EU-style. Up until the beginning of the year 2012, the world had 89 countries with data privacy laws.[1] Outside the EU (27 countries) and EEA (3 countries), where the European Directive 95/46/EC is binding, there were a total of 59 countries with data protection laws in Europe, Asia, Latin America, Africa, Middle East, the Caribbean, North America and Australasia.[2] Africa has 11 countries out of 54 with such legislation while about eight others have either prepared draft or concrete bills. The latter are still pending before their executive or legislative bodies. Commentators in the field of data privacy are in agreement that the adoption of data protection legislation outside of Europe is largely a result of the influence of the European regime of data protection. Such regime is mainly comprised under the EU Directive 95/46/EC. They assert that the Directive is the most influential instrument of all international codes of data protection policies in the world.[3] This influence, unlike the rest of the international codes such as the OECD Guidelines 1980, Council of Europe Convention 1981 and UN Guidelines 1990, originates mainly from the Directive's spill-over effect. To be sure, Article 25 of the Directive clearly restricts transfer of personal data from EU/EEA to third countries if such countries do not provide an 'adequate' level of protection of personal data. What this means is that third countries which are non-EU/EEA countries have to enact data protection legislation that must be considered by Europe as adequate if they wish to receive personal information from residents in EU/EEA. Because of Article 25 of the Directive, Europe has been criticised for legislating for the whole world. Indeed, the European Union itself through the Article 29 Working Party has expressed fears with regard to an assessment of the 'adequacy' of data protection in third countries as this may amount to an act of political provocation of sovereign states risking to spoil diplomatic relations. In their view 'some third countries might come to see the absence of a finding that they provided adequate protection as politically provocative or at least discriminatory, in that the absence of a finding is as likely to be the result of their case not having been examined as of a judgment on their data protection system.'[4] Amplifying this fear Seth Hobby posits that 'no country likes to feel the downward pressure of being dictated to concerning issues that may have significance in terms of a nation's ability to regulate its own affairs, ergo national sovereignty, simply because of economic leverage.'[5] Yet in an attempt to minimise or remove these fears, Europe has cautiously left it to third countries to initiate the process of 'adequacy' assessment. Indeed, the fact that it would be difficult for all third countries to meet the 'adequacy' standard prompted Europe to incorporate Article 26 in its regime to permit continued transfer of personal data from the EU/EEA to third countries that fail to meet the 'adequacy' test of the European law. In the latter case, some minimum criteria less stringent than the requirement of Article 25 must first be fulfilled. This allowance strategically helps

1 Greenleaf, G., 'Global data privacy laws: 89 countries, and accelerating', Queen Mary University of London, School of Law Legal Studies Research Paper No. 98/2012.

2 Ibid, p.5. Note that the number of countries with data protection laws outside Europe has kept increasing since 2012 with for example Ghana adopting data privacy legislation in February 2012.

3 See e.g., Kuner, C., 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', TILT Law & Technology Working Paper No. 016/2010 October 2010, Version: 1.0, p.6, Social Science Research Network Electronic Paper Collection, at p. 9.

4 Article 29 Data Protection Working Party, 'Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive', DG XV D/5025/98/WP 12, (adopted on 24th July 1998), p. 27.

5 Hobby, S.P., 'The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U.S Position has progressed', International Law & Management Review, 2005, Vol. 1, pp.155-190, at p.159.

Dr. Alex B. Makulilo

Lecturer, Faculty of Law, Open University of Tanzania

E-Mail: alex.makulilo@out.ac.tz

Europe to transfer personal data to its trading partners at least at a limited level. Undoubtedly Africa, with its eleven countries so far with comprehensive data protection legislation, largely relies on Article 26 of the Directive to trade with Europe.

It is worth noting that the 'adequacy' standard in Article 25 of the Directive has drawn European and its counterpart American scholars into a fierce debate as to whether it is proper for Europe to adopt a data protection regime with sweeping effect. This debate had and still has impact in the development of data protection policies on the two sides of the Atlantic and beyond such regions. This article is set to investigate the place of Africa in the trans-Atlantic debate and assess its overall implication to the data protection reforms in the continent.

2 The trans-Atlantic debate

The trans-Atlantic debate over the protection of personal data traces its origin from the adoption of the European Directive 95/46/EC in 1995. Such debate is premised on modes of regulating privacy. Traditionally, Europe has regulated privacy by comprehensive legislation for a long time. The main features of such a regulatory regime are the incorporation of the basic principles of data protection as well as supervisory authorities. These authorities have the primary obligation to enforce the basic principles of data protection and incidental matters. In contrast, the US have only invoked an *ad hoc* sectoral approach. Under this regulatory approach, the market has been left to regulate the private sector with a multitude of privacy legislation while a sort of 'comprehensive' legislation covers the public sector only. Unlike in Europe, the United States' legislative approach lacks a set of basic data protection principles as well as a centralised supervisory authority.

The bottom-line of the differences between EU and US regulatory approaches to protection of privacy are two opposing philosophies. For Europe, the comprehensive approach is largely informed by human rights sentiments that were a result of the traumas of the World Wars. Indeed, the rise of the norm of 'dignity' which is at the core of privacy in Europe is a product of a reaction against fascism and especially against Nazism.[6] In this way privacy is protected as a fundamental human right in Europe. To be sure, Article 8 and 17 of the European Convention on Human Rights and Fundamental Freedoms 1950 and International Covenant on Civil and Political Rights 1966 respectively provide the normative basis of data protection in Europe. These two provisions and case law developed around them have been the subject of wide academic discussion.[7] In contrast, the American philosophy of privacy is built upon the norm of 'liberty' of individuals in relation to the state.[8] Hence, in 1890 Samuel Warren and Louis Brandeis published their seminal article '*The Right to Privacy*'[9] in which they reflect on the American views to privacy as the 'right to be let alone'.

Despite the regulatory difference between Europe and America, there had never been any stronger debate across the Atlantic in the period preceding the Directive 95/46/EC. This is partly because first, the codes of data protection existing prior to the Directive were only soft law (e.g. OECD Guidelines 1980, Council of Europe Convention 1981 and UN Guidelines 1990) and as such not binding. Secondly, none of these codes provided a restrictive regime of the international transfer of personal data as it is the case with the Directive 95/46/EC which unlike the previous codes is binding. As pointed out, it was formally in 1995 that the trans-Atlantic debate emerged. On behalf of the US, Seth Hobby argues that 'although the primary goal of the Directive was to inculcate unity of data protection regulation among the states of Union (then numbering fifteen), certain provisions (particularly Article 25) contained within the Directive dealing with data transfers to countries outside of the EU have an absolute impact on the data protection policies of every nation that trades with an EU member.'[10] He further argues that 'given that at the inception of the Directive no single nation in the world had a data protection framework even remotely close to that required by EU's mandate, such a requirement automatically injected the international community with a dose of insecurity over its future trade potential with the EU.'[11] Seth concludes that 'when considered in a broad global context, it is hard to avoid the feeling that the EU's implementation of such a wide sweeping regulatory exercise in the realm of fundamental human rights goes far by effectively creating a world-wide data privacy utilizing the proverbial back door.'[12] Seth's stance has frequently recurred in America's scholarship in various ways. Because of this, the present article avoids repetitions of each and every formulation of America's side of arguments.

At the same time, some of the US discussion against the long arm of Directive 95/46/EC has focused on the legality of the provisions under international trade law, most notably the 1994 General Agreement on Trade in Services (GATS) which restricts signatory states from limiting transborder data flow in ways that involve arbitrary or unjustified discrimination against other states.[13] Nevertheless, such prohibition is not absolute. By way of exception to the general rule, GATS allows under Article XIV(c) (ii) minimum restriction on transborder data flow in order to secure 'protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.' Bygrave argues that while such restrictions must also conform to the Agreement's basic prohibition against arbitrary or unjustified discrimination between countries and against disguised restrictions on trade in services, little if any solid evidence indicates that Article 25 and 26 of the Directive have been or are being applied in breach of that prohibition.[14]

6 Beignier, B., Le Droit de la Personnalité 60-61 (1992) cited in Whitman, J.Q, 'The Two Western Cultures of Privacy: Dignity versus Liberty', The Yale Law Journal, 2004, Vol.113, pp.1151-1221 at 1166.

7 See e.g. Bygrave, L.A., 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', International Journal of Law and Information Technology, 1998, Vol.6, No.3, pp.247-284; Ulyashyna, L., 'Does case law developed by the European Court of human Rights pursuant to ECHR Article 8 add anything substantial to the rules and principles found in ordinary data protection principle?', A Tutorial Paper presented at the Norwegian Centre for Computers and Law (NRCCL), Spring, 2006; De Hert, P and Gutwirth, S., 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action', in Gutwirth, S *et al* (eds)., Reinventing Data Protection?, Springer, 2009, pp.3-44.

8 Buchner, B., Informationelle Selbstbestimmung im Privatrecht, 2006, pp. 19-20.

9 Warren, S.D and Brandeis, L.S., 'The Right to Privacy', Harvard Law Review, 1890, Vol. 4, No.5, pp.193-195; for German translation see Datenschutz und Datensicherheit (DuD), 2012, Vol. 36, pp. 755-766.

10 Hobby, p.156, note 5, supra.

11 Ibid, p.157.

12 Ibid.

13 Bygrave, L.A., 'International Agreements to Protect Personal Data' in G. Greenleaf and J.B. Rule (eds)., Global Privacy Protection: The First Generation, Edward Elgar Publishing Limited, Cheltenham,UK/Northampton, MA,USA, 2008, pp.15-49, at p. 40.

14 Ibid, p.41.

Similarly, allegations have been raised to the effect that by adopting Directive 95/46/EC, Europe intended to protect its business interests against the whole world. There are no absolute rejections of these allegations and Bygrave argues convincingly that it is scarcely to be overlooked that implementation of the Directive – particularly of Arts 25 and 26 – might well have protectionist benefits for data controllers established within the EU.[15] This position is in line with the view taken by Justice Michael Kirby, Chairman of the expert group responsible for drafting the OECD Guidelines which are similar to Directive 95/46/EC, that such a policy was adopted for purposes of economic protectionism.[16]

For Europeans, it has widely been viewed that the United States of America's approach to protection of privacy is a weak standard. Moreover, Europe has defended its comprehensive regime of data privacy and in particular Articles 25 and 26 of the EU Directive 95/46/EC as a means to ensure that personal data of its citizens and residents are not relocated to off-shore destinations without adequate protection of personal data rendering the Directive impotent.

Appreciating the differences in regulatory approaches to data protection and in attempting to reconcile the tension over the trans-Atlantic debate, the EU and the US forged the *Safe Harbor (SH)* arrangement. The latter was adopted in the year 2000. Essentially the SH comprises privacy principles in a modified and simplified version that are applied by companies on both sides of the Atlantic when transferring personal data. Although the EU Commission had decided that the SH meets the adequacy test of European law, SH is an arrangement that Europe is not comfortable with. It is arguable that the European Commission's adequacy decision on SH was passed for the convenience of a continued flow of personal data on both sides of the Atlantic with the view of sustaining trade, but falls considerably below the Directive's standards. The strong criticism of this low standard by other European bodies (e.g. Article 29 Working Party) means that it is no exaggeration to say that the Commission had sold out Europe's high privacy standards set by the Directive in order to protect its US trade.[17] It has been argued that the SH decision could signal that the EU Commission will decide that weak privacy protection in other countries is also 'adequate' to avoid accusations of inconsistency and hypocrisy.[18] Yet this may not necessarily be the case taking into account the fact that the SH was negotiated between two powers with relatively equal economic strength and different, but long-established traditions of protection of privacy. It is difficult to imagine that Europe will be prepared to negotiate another SH with other countries, especially developing countries whose economies are weak.

With the adoption of the SH the initial tension between the USA and EU in the wake of the Directive's adoption cooled considerably.[19] However, the EU's proposed new data protection regulation announced on 25 January 2012 has provoked afresh the trans-Atlantic debate. This can be demonstrated, for example, by the conference organised by the European Commission in Washington in the spring of 2012 which saw tit-for-tat exchanges between EU and US government representatives as to which of them have the better system.[20] It is worth noting that the US' efforts to regulate privacy culminating in the adoption of the Commercial Privacy Bill of Rights 2011(later renamed Consumer Privacy Bill of Rights 2012) have been severely criticised. For example, in her speech towards the end of the year 2011, Viviane Reding (the Vice-President of the European Commission, EU Justice Commissioner) openly criticized the U.S Commercial Privacy Bill of Rights as the U.S 'self-regulation' may not be sufficient to achieve full interoperability between the EU and U.S.[21] This comment clearly indicates that the trans-Atlantic debate will not end any time soon.

3 Beyond the trans-Atlantic debate: Africa's perspective

The dominant view in privacy literature is that Africans do not have or value privacy. The single reason advanced by scholars is that the over-dominance of collectivist cultures in African societies outweighs the self-autonomy of individuals and hence denies them space to claim for privacy.[22] However, a departure from the dominant school of thought is noticeable in the stance taken by Professor Nwauche who asks, 'is privacy important in Nigeria?' He answers this question affirmatively, advancing the reason that there are human beings in Nigeria and more so a constitutional protection of this right. Yet, he notes that this is one right that has not received adequate protection or elaboration both in the definition, philosophical basis or the key issues of the concept of privacy.[23] Accordingly, Nwauche associates the existence of privacy values in Nigeria and probably across Africa with the dignitary concept which seeks to protect the personality of an individual because he is a human being.[24]

Likewise some African scholars have struggled to conceptualise privacy in the African cultural context in vain. For instance, Bakibinga has made a fruitless call that 'privacy has to be defined in a way that is acceptable to the Ugandan society given the emphasis on communalism versus individual rights.'[25] To achieve that, Bakibinga recommends that one way to start seeking for such definition would be to commission studies to obtain perceptions of privacy within the Ugandan society.[26] Interestingly, the only attempt made so far to define privacy in Africa, though still patterned to the Western culture, is that of Professor Neethling. His theory states that 'privacy is an individual condition of life characterised by exclu-

15 Bygrave, L.A., Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer Law International, the Hague/London/New York, 2002, p.115.

16 Kirby, M.D., 'Legal Aspects of transborder data flows', International Computer Law Adviser, 1991, Vol.5, No.4, pp.4-11, at pp.5-6.

17 Greenleaf, G., 'Safe Harbor's Low Benchmark for "adequacy": EU sells out Privacy for US$', PLPR 32, http://www.austlii.edu.au/au/journals/PLPR/2000/32.html accessed 31 March 2013.

18 Ibid.

19 Bygrave, note 12, supra.

20 Kuner, C *et al.*, 'The end of the beginning' International Data Privacy Law, 2012, Vol.2, No.3, pp.115-116, at p.116.

21 Reding, V., 'The Future of Data Protection and Transatlantic Cooperation', Speech at the 2nd Annual European Data Protection and Privacy Conference (SPEECH/11/851), Brussels, 6 December 2011, pp. 1-4, at p.4; see also, Greenleaf, G and Waters, N., 'Obama's Privacy Framework: An offer to be left on the table?' Privacy Laws & Business International Report, 2012, No.119, pp.6-9.

22 See e.g., Gutwirth, S., Privacy and the Information Age, Lanham/Boulder/New York/Oxford/ Rowman & Littlefield Publ., 2002, p.24; Bygrave, L. A., 'Privacy Protection in a Global Context – A Comparative Overview', Scandinavian Studies in Law, 2004, Vol. 47, pp. 319–348, at p.328; Bygrave, L.A., 'Privacy and Data Protection in an International Perspective', Scandinavian Studies in Law, 2010, Vol. 56, pp.165-200, at p.176.

23 Nwauche, E.S., 'The Right to Privacy in Nigeria', Review of Nigerian Law and Practice, 2007, Vol.1, No.1, pp.62-90, at p. 66.

24 Ibid, p.65.

25 Bakibinga, E. M., 'Managing Electronic Privacy in the Telecommunications Sub-Sector: The Ugandan Perspective', 2004, http//:thepublicvoic.org/eventscapetown04/bakibinga.doc, pp.1-13, at p.12.

26 Ibid, p.13.

sion from publicity. This condition includes all those personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy.'[27] That far, it can safely be argued that privacy in Africa is principally an imported Western liberal concept. Bakibinga convincingly posits, that although in Africa the community comes first, privacy will still be an important concern as the information technology revolution advances.[28] On the other hand, it may be argued that at present many Africans largely suffer from 'privacy myopia' i.e. the tendency to undervalue the bits of information about themselves so that it does not seem worth it to go to the trouble of protecting such information.[29]

Not surprisingly therefore, privacy reforms in Africa continue to take shape at a snail's pace. This is despite the restrictions of the transfer of personal data to third countries put under Article 25 of the EU Directive 95/46/EC. It is imperative to point out that the pressure generated so far on the United States by the European data privacy regime has at present not yet arisen in a direct and serious manner in view of the fact that African countries just like many other developing countries are not major trading partners of the EU Member States.[30] Yet, those few African jurisdictions which have so far adopted data protection legislation have largely done so for economic motivations though. The rest of African countries without data protection legislation rely upon the exceptions permitted under Article 26 of the Directive to exchange personal information with the EU. This explains why, for example, South Africa was able to accommodate the 2010 World Cup at the time when massive personal information of EU citizens was being transferred to South Africa despite the fact that she had no data protection legislation.

Although the current sub-regional privacy codes in Africa such as ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection for the Economic Community of West African States, the SADC Data Protection Model Law 2012 for Southern African Development Community and the proposed draft African Union convention on establishment of a credible legal framework for cyber security in Africa 2011 are likely to influence the development of data protection law in Africa,[31] doubts have been cast on their ability to do so. The proposed Nigerian data protection bill is a case at point. This bill is a far weaker standard than the ECOWAS Supplementary Act which is binding code in Nigeria, an ECOWAS member.[32] There is also little evidence that suggests that the adoption of data protection legislation in the eleven African countries was/is in compliance with sub-regional data privacy codes in Africa. This is because, first, most of the national data protection legislation in Africa pre-dates such codes. Second, even after the adoption of these sub-regional codes little or no adjustments have been made in the national data privacy legislation in line with them. It is also interesting to note that national laws on data protection in Africa which post-date the sub-regional data protection codes make little or no reference to such sub-regional codes. This is the case for example with South Africa, where the preparatory works to the proposed Protection of Personal Information Bill 2009 show no reference to the SADC Data Protection Model Law (to which South Africa is a SADC member state). Interestingly, the reference point to the South African proposed law has been at all the times the EU Directive 95/46/EC and even the draft EU proposed Data Protection Regulation announced on 25 January 2012 which is not yet adopted.

At the same time it is worthwhile to point out that the African sub-regional, regional as well as national data protection legislation are all modelled upon the European Directive 95/46/EC. This is because it is the desire of African countries to meet the 'adequacy' standard of the European law so as to attract foreign investments. Yet, the recent assessments by EU led consultants of the four African jurisdictions namely, Burkina Faso, Mauritius, Tunisia and Morocco reveals that they are still far away from the EU 'adequacy' standard.[33] Nevertheless, the EU Directive remains the most preferred model of privacy regulation in Africa. Perhaps the question is whether Africa adapts the EU model of privacy regulation through conscious choices or forceful imposition by Europe? In other words, has the trans-Atlantic debate or anything of the nature of such debate emerged in the course of the data protection law reforms in Africa?

Up until recently, there has been a lack of serious academic debate among African scholars critical of the European extra-territorial reach of the EU Directive 95/46/EC. There are also no prospects for this debate to arise as more African countries enact data privacy legislation in the EU-style. Concomitantly African commentators have taken a positive view of the EU model of data protection. There is little feeling that EU is imposing its data protection regime as is the case with the trans-Atlantic debate where American scholars are bitter about the EU data protection regime. So far, the majority of scholars in Africa positively recommend the adoption of data protection legislation based on the EU model. For instance, Neethling asserts that with the exception of Van der Merwe, South African commentators are unanimous that the creation of such measures (data protection) through legislation is a matter of great urgency.[34] Similarly, calls by other commentators in Africa for adoption of data protection legislation in the EU style include Ubena;[35] Kusamotu;[36] Izougu;[37] Nwanko;[38]

27 Neethling, J., 'The Concept of Privacy in South African Law', The South African Law Journal, 2005, Vol.122, No.1, pp.18-28, at p.19.

28 EPIC Alert, 'EPIC Hosts Privacy and Public Voice Conference in Africa', 23 December 2005, Vol. 11, No. 24, http://www.epic.org/alert/EPIC_Alert_11.24.html accessed 31 March 2013.

29 See e.g., Bakibinga, p.5, note 24, supra.

30 Carauna, M.M and Cannataci, J.A., 'European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States', Information & Communications Technology Law, 2007, Vol. 16, No. 2, pp.99-124, at p.110.

31 See e.g., Greenleaf, p.8. note 1, supra.

32 Makulilo, A.B., 'Nigeria's Data Protection Bill: Too many surprises,' Privacy Laws & Business International Report, 2012, No.120, pp.25-27.

33 For detailed analysis of these assessments, see e.g., Makulilo, A.B., 'Data Protection Regimes in Africa: too far from European 'adequacy' standard?,' Journal of International Data Privacy Law, 2012, Vol.3, No.1, pp.42-50.

34 Neethling, J *et al.*, Neethling's Law of Personality, 2nd Edition, LexisNexis, Durban, 2005, p.271.

35 Ubena, J., 'Tanzania lag on privacy law', Tanzania Legal News, posted on 8th June 2010, http://tanlex.wordpress.com/ accessed 02 April 2013; see also, Ubena, J., 'Privacy: A Forgotten Right in Tanzania', the Tanzania Lawyer, 2012, Vol.1, No.2, pp. 72-114.

36 Kusamotu, A., 'Privacy Law and Technology in Nigeria: The Legal Framework will not meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46', Information & Communications Technology Law, 2007, Vol.16, No. 2, pp. 149-159.

37 Izuogu, C.E., 'Data Protection and Other Implications in the Ongoing SIM Card Registration Process', 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665, accessed 02 April 2013; see also Izuogu, C.E., 'Nigeria: Data Protection & Privacy Issues in NCC's Directive on SIM Card Registration', 2010, http://www.facebook.com/note.php?note_id=388277770826 accessed 02 April 2013.

38 Nwanko, I.S., 'Part I: Nigeria's SIM Card Registration Regulations 2010: The Implications of unguarded Personal Data Collection', http://www.facebook.com/note.php?note_id=10150095718055827 accessed 02 April 2013; see also Nwanko, I.S., 'Part II: Nigeria's SIM Card Registration Regulations 2010: The Implications of

Akinsuyi;[39] Enyew;[40] and Bakibinga.[41] At the same time, commentators who have not recommended the adoption of data protection legislation based on EU model have done so not because they feel that the EU regime is imposed on their respective countries or Africa but rather because they believe that common law is sufficient to protect privacy in their respective countries.[42]

The acceptability of the EU data protection model in Africa was/is further accentuated by other factors. First and foremost is that while on its face privacy appears to be incompatible with African cultural values (i.e. *ubuntu)*, such culture has less strong expression and philosophy in the privacy arena. As a result, *ubuntu* cannot guide or influence legislation significantly more than for example the EU Data protection principles.[43] However, this can be contrasted with other aspects of African culture which are not only incompatible to Western culture, but also significantly capable of influencing legislation. The case at point is, for instance, the contentious issue surrounding homosexuality in the African culture. While in many parts of sub-Saharan Africa homosexuality is generally illegal reflecting African culture, recent wrath by African governments against Western attempts to compel such governments to legitimise homosexuality amid threats of cutting aids has seen the adoption or proposals for adoption of anti-homosexuality laws. The famous 'Kill the Gays Bill' in Uganda is illustrative.

At the same time, the major legal systems in Africa namely common and civil law legal systems which are Western in origin, create fertile grounds for adaptability of European law. While these systems were forcibly imposed on Africa by European countries during colonial rule as part of the colonial superstructure and an instrument of coercing Africans to participate in the colonial economy, they were inherited by African countries on independence. For example, in many common law jurisdictions, common law, doctrines of equity and statutes of general application in the United Kingdom are still the sources of municipal law.[44] Thus, the attitude to view these systems as colonial has diminished significantly as more customisation continues to take place. It is arguable that African countries are no strangers to the adaptation of 'foreign law'.

The role of international law is also significant. Oppong, while citing other commentators, underscores that 'Africa is becoming more "international law-friendly"'.[45] He goes on to posit that 'the initial hostility or ambivalence of the post-colonial towards international law is giving way to increased participation in international law processes, both in terms of institutional participation and in the development of norms.'[46] This can be demonstrated by the frequent trend in Africa towards making international law supreme over and directly or automatically applicable within the domestic legal systems.[47] Concomitantly, the concept of sovereignty, which suggests that national legal systems are sealed or isolated from outside interference, is being re-assessed.[48]

Similarly, there is the role of judiciary in Africa in interpreting new areas of law influenced by modern technologies. In *Trust Bank Tanzania Ltd v. Le-Marsh Enterprises Ltd and Others*,[49] for example, the High Court of Tanzania while interpreting whether a computer printout is a banker's book, made the following observations '...Tanzania is not an island by itself. The country must move fast to integrate itself with the global banking community in terms of technological changes and the manner in which banking business is being conducted. The courts have to take due cognizance of the technological revolution that has engulfed the world. Generally speaking as of now, record keeping in our banks is to a large extent "old fashioned" but changes are taking place. The law can ill afford to shut its eyes to what is happening around the world in the banking fraternity.' These remarks justified the court to use the UK Banking Act 1979 to fill the gap in the Tanzanian Evidence Act, Cap 6 R.E 2002 and held that a computer printout amounted to a banker's book. It is worth noting that in an earlier case of *Tanzania Cotton Marketing Board v. Cogecot Cotton Company SA*,[50] the Court of Appeal of Tanzania (the Supreme Court), held that the words 'registered post' appearing in Rule 4 of the Arbitration Rules, 1957 should be interpreted widely enough in order to take into account the current development in communication technology that has taken place since 1957 when the rules were enacted. The approach taken by Tanzanian courts with regard to legal interpretation in the context of modern technologies is similar to that of other sub-Saharan countries. It is arguable that since privacy risks are accelerated by modern technologies, courts in Africa will be likely to incline towards applying foreign law in deciding privacy disputes.

4 Final remarks

If anything, data protection reforms in Africa have been largely influenced by the Directive 95/46/EC. In all eleven countries which have so far adopted omnibus data protection laws, the legislative processes indicate that the broad agenda of these legal reforms is to sustain business process outsourcing from Europe. Indeed Article 25 of the Directive is frequently cited as the justification for adopting data protection laws in Africa. Be as it may, the data protection law reforms in Africa have not been accompanied by a rejectionist debate such as the trans-Atlantic policy debate. In contrast, African scholars have scarcely raised any alarm as to the Directive's regulatory overreaching. Rather they have been positive about the EU data protection model and have even encouraged their governments to adopt comprehensive data protection legislation. It is submitted that in Africa the trans-Atlantic policy debate is more of academic relevance than a practical one with real implications for Africa's data protection law reforms. The EU Directive is widely viewed as the source of inspiration, comparative law, and model in African legislative reforms.

unguarded Personal Data Collection', http://www.facebook.com/note.php?note_id=10150095718055827 accessed 02 April 2013.

39 Akinsuyi, F.F., 'Data Protection Legislation for Nigeria, The Time is Now!', Nigerian Muse, http://www.nigerianmuse.com/20071004075550zg/sections/general-articles/data-protection-legislation-for-nigeria-the-time-is-now/ accessed 02 April 2013.

40 Enyew, A.B., 'Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia', LL.M Thesis, University of Oslo, Norway, 2009.

41 Bakibinga, note 25, pp.12-13, supra.

42 Nwauche, note 23, p.83, supra.

43 Olinger, H.N, *et al.*, 'Western privacy and/or Ubuntu? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa', the International Information & Library Review, 2007, Vol. 39, No. 1, pp. 31-43, p.40.

44 See e.g., Tanzanian Judicature and Application of Laws Act, Cap.358 R.E 2002, s. 2(3).

45 Oppong, R.F., 'Re-imagining International Law: An Examination of Recent Trends in the Reception of International Law into National Legal Systems in Africa', Fordham International Law Journal, 2006, Vol.30, No.2, pp.296-345, at p. 296.

46 Ibid.

47 Ibid, p.297.

48 Ibid, p.326.

49 [2002]T.L.R 145, at pp.148-149.

50 [1997]T.L.R 165, at p.170.