Privacy and data protection in Africa: a state of the art

Alex Boniface Makulilo*

Abstract

- A literature review is pivotal to any scientific research or writing. Quite often a prudent researcher may not embark on research or writing a scientific piece of work without first reviewing the literature. Yet this literature may sometimes not be readily available, especially in a relatively new area of scholarship, or its availability may be challenging.
- In this article I survey the major literature on privacy and data protection in Africa as an emerging field of law.
- I argue that currently this literature is underdeveloped.
- I offer a modest proposal that efforts have to be directed towards training, researches, networking, the creation of modern libraries, inter-country/sub- or regional discussions and establishing journals specifically dedicated to privacy and data protection law issues.

Introduction

After about forty years of development of data privacy law in the world, at last Africa has slowly started to be involved in the discourse. In the last decade Africa witnessed the development of nine enactments on data privacy in Cape Verde (22 January 2001), Seychelles (24 December 2003), Burkina Faso (20 April 2004), Mauritius (17 June 2004), Tunisia (27 July 2004), Senegal (15 January 2008), Morocco (18 February 2009), Benin (22 May 2009), and Angola (17 June 2011). Other countries have Bills on similar law pending before their legislative bodies (Ghana, Ivory Coast, Kenya, Madagascar, Mali, Niger, and South Africa) or are still discussing drafts of such laws in various fora according to the legislative traditions of respective countries. It is imperative to mention that this development is largely due to the inertia of the European Directive 95/46/EC. The latter requires that any transfer of personal data to third countries (ie non-European Union/EEA member states) must provide an adequate level of data protection. Since African countries are third countries to Directive 95/46/EC they are subject to this clause. The other reason that has provided an environment for the development of data privacy law in Africa is the rapid development of information and communications technologies in the continent. Yet, despite this legislative development, literature on data privacy in Africa has remained scant, fragmented, and has continued to grow at a snail's pace. This article intends to situate the contours of this literature to uncover its nature, quality, the scope of issues addressed, and existing impediments inhibiting its growth. It also aims to recommend strategies to improve the situation of this scholarship.

The contribution of this article is particularly important in four main ways. By consolidating a fairly comprehensive listing of the major literature, the article provides researchers with easily accessible information on the privacy and data protection literature in Africa. While this information is likely to be more beneficial to comparative researches or studies, at the same time it offers a useful starting point for a background review for non-comparative research or studies. Also important, this article provides, though more generally, an overview of the current state of systems of privacy and data protection policies and regulations across Africa. In addition, it identifies the specific issues which have so far been addressed by this literature and in so doing, it hints at which issues are currently under-researched

* Alex B. Makulilo is currently a PhD student at the Faculty of Law, University of Bremen (Germany). I am particularly indebted to all who made available to me their scholarly works. In particular I wish to thank the following: Associate Professor Lee A. Bygrave, Professor Graham Greenleaf, Professor Iain Currie, Professor Anneliese Roos, Mr. David Banisar, Professor Serge Gutwirth, Mr. João Luís Traça, Mr. Bernardo Embry, Mr. Ewan Sutherland, and Mr. Stephen Kaduuli.

or not researched at all. Accordingly, researchers may wish to focus on such issues for their future research agendas. Finally, this article may serve as the catalyst for the networking of experts by identifying who has researched what, where, when, and why.

Conceptual framework

Privacy and *data protection* are two contentious concepts in the discourse of privacy. It is loosely assumed that the two concepts belong to the two sides of the Atlantic. While the term *privacy* is widely used in the USA the term *data protection* is commonly used in European jurisdictions instead.[1] Yet this territorial use of the two terms is problematic for two reasons. First, it fails to distinguish the inherent similarities and differences between these concepts. Second, at some point both-terms find their way to the opposite side of the Atlantic, and henceforth exist simultaneously side-by-side.

Some commentators tend to view privacy and data protection as synonymous and the terms interchangeable. Yet others have maintained the opposite view. Cuijpers raises a question, 'is the right to data protection the same as the right to privacy?'[2] In response he concurs with Peter Block that *data protection* and *privacy* are not the same. Cuijpers argues that, since an individual right to privacy safeguards an undisturbed private life and offers the individual control over intrusion into the private sphere, it is different from protection of the individual with regard to the processing of personal data which is not restricted to the private sphere of the individual.[3] In the same vein De Hert and Gutwirth argue that 'data protection's real objective is to protect individual citizens against the unjustified collection, storage, use, and dissemination of their personal details. This objective seems to be indebted to the central objective of the right to privacy, to protect against unjustified interference in personal life. Many scholars therefore hold data protection and privacy to be interchangeable.'[4] Yet in refuting the above view, they argue that equating *privacy* and *data protection* on the basis of the objectives each wants to achieve is a narrow view. To the contrary, De Hert and Gutwirth hold that there are important differences between the two in terms of scope, goals, and content.[5] By subscribing to Bygrave's views extracted from his article, *The Place of Privacy in Data Protection Law*,[6] De Hert and Gutwirth continue to argue that while privacy obviously occupies a central place in data protection law, their characterization of data protection law as solely or even essentially concerned with safeguarding privacy is misleading.[7] Data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualizations of privacy.[8]

The difficulty of defining privacy and data protection has at times led to frustrated commentators failing to clearly point out the differences between the two concepts. For example, Kuner argues that *privacy* can be seen as a concept which is both broader than and independent of *data protection*, although there can be a significant overlap between the two.[9]

Somewhat confusingly, De Hert and Schreuders argue that although the terms *data protection* and *privacy* share certain features and goals, and are frequently used as synonyms, they are not identical.[10] They are therefore described as being 'twins, but not identical'.[11] These scholars argue that, although clearly ingrained in privacy protection, *data protection* does not necessarily raise *privacy* issues.[12] Contrary to privacy rules, data protection rules are not prohibitive.[13] Instead they organize and control the way personal data can only be legitimately processed if some conditions pertaining to the transparency of the processing, the participation of the data subject, and the accountability of the data controller are met.[14]

Yet, between the two ends of the spectrum, there are commentators who, in an attempt to reconcile the opposing views, have invented the new concept *data*

1 LA Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International, The Hague/London/New York 2002) 1.

2 C Cuijpers, 'A Private Law Approach to Privacy: Mandatory Law Obliged?' (2007) 4/4 SCRIPTed 304–18, at 312.

3 Ibid.

4 P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action', in S Gutwirth, *et al.* (eds), *Reinventing Data Protection?* (Springer, New York 2009) 3–44, at 3.

5 Ibid, at 9.

6 LA Bygrave, 'The Place of Privacy in Data Protection Law' (2001) 24/1 University of New South Wales Law Journal 277–283, at 282; available at <http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html> accessed 26 February 2012.

7 De Hert and Gutwirth (n 4), at 10.

8 Ibid.

9 C Kuner, 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 Computer Law & Security Review 307–317, at 308.

10 P De Hert and E Schreuders, 'The Relevance of Convention 108', 33, 42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19–20 November 2001 cited in *EU Study on the Legal Analysis of a Single Market for the Information Society*, DLA PIPER, UK, November 2009, ch. 4, at 4.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

privacy.[15] Bygrave argues that in contrast to the concept of *data protection* which fails to indicate the central interests served by the norms to which it is meant to apply, *data privacy* is more appropriate as it better communicates the central interest(s) at stake and provides a bridge for synthesizing North America and European policy discussion.[16] Closely similar to Bygrave other commentators tend to use the concept *information privacy* instead for the above discussed sense. Karanja, for example, argues that

> the concept '*information privacy*' is concerned with the protection of personal data. In Europe, the term "data protection" is used to refer to 'information privacy'. Although the two concepts, information privacy and data protection, may differ somewhat in meaning and the scope of the former being wider than the latter (sic). Both expressions are used interchangeably to refer to the same thing—protection of personal data.'[17]

Attempts to demarcate the realm of *privacy* from that of *data protection* have also been made using the case law of the European Commission and Court of Human Rights (ECtHR) interpreting the right to privacy enshrined in Human Rights Treaties. The latter include Articles 17 and 8 of the International Covenants on Civil and Political Rights (ICCPR) 1966 and the European Convention for the Protection of Human Rights and Fundamental Freedoms(ECHR) 1950 respectively. Although there seems to be consensus among commentators on the limitations of the Strasburg privacy case law in spelling out data protection principles, the reasoning has varied significantly. For example, in summing the limited scope of the Strasburg case law in relation to data protection, Bygrave argues:

> at present, the case law developed around the right to privacy in Article 17 of the ICCPR and Article 8 of the ECHR falls short of explicitly stipulating data protection guarantees as comprehensive as those found in instruments concerned specifically with data protection. Moreover, the case law is somewhat confusing: the principles for processing personal data which emerge from it are often sketchy and of little prescriptory value. This is so even with the relatively extensive body of case law developed around Article 8 of the ECHR. Too often there has been failure by the Commission and/or Court to make clear exactly which elements of the contested data processing practice has interfered with the right under Article 8(1); too often has there been a concomitant failure to describe the threatened interest.[18]

However, Bygrave notes that the omitted prescriptory value of Article 8 case law in the field of data protection is not simply due to the Commission and Court.[19] It is also due to the fact that a large proportion of the case law concerns data processing in a rather special context (ie, secret surveillance activities by police or intelligence agencies), while almost none of it deals with private entities' data processing practices.[20] Notwithstanding all these limitations, Bygrave was optimistic about the willingness of the Strasbourg organs to adopt data protection provisions which grow nationally and internationally, and that these organs will increasingly expand the right to privacy in the light of these laws.[21] Bygrave's optimism was borne out seven years later by Karanja in his analyses of the case law of the ECtHR. Summarizing the value of this case law in relation to data processing practices Karanja argues:

> Going by the recent case decisions of the ECtHR, it is no longer doubtful that data protection is a human right although the Convention does not state this. As indicated above, the Court has boldly manifested data protection principles in its decisions by adopting the language of data protection law. But what still lacks in the Council of Europe human rights framework is a positive statement in the general human rights legislation that human rights protects personal data. Such statement would give data protection the universal status enjoyed by human rights principles. The EU has cured the anomaly by enacting a data protection provision in its Charter of fundamental rights and the EU Constitution.'[22]

It is noteworthy that the above view by Karanja are in sharp contrast to the observation of the European Court of First Instance in *Bavarian Lager Co. Ltd v Commission*.[23] In this case, the Court observed, 'it should also be emphasized that the fact that the concept of "private life" is a broad one, in accordance

15 PM Schwartz and JR Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (Michie Law Publishers, Charlottesville 1996) 5.

16 LA Bygrave, 'Privacy Protection in a Global Context—A Comparative Overview' (2004) 47 Scandinavian Studies in Law 319–48, at 321–2.

17 SK Karanja, 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation', PhD Thesis, Faculty of Law, University of Oslo, (2006) 86.

18 LA Bygrave, 'Data Protection Pursuant to the Right in Human Rights Treaties' (1998) 6/3 International Journal of Law and Information Technology 247–84, at 283–4; see also, L Ulyashyna, '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).

19 Bygrave (n 18).

20 Ibid, at 284.

21 Ibid.

22 Karanja (n 17), at 123.

23 Case T-194/04 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004A0194:EN:HTML> accessed 26 February 2012. Judgment was delivered at Luxembourg on 8 November 2007.

with the case-law of the European Court of Human Rights, and that the right to the protection of personal data may constitute one of the aspects of the right to respect of private life … does not mean that all personal data necessarily fall within the concept of "private life"'.[24] Moreover, De Hert and Gutwirth have more recently critically evaluated the case law of Strasbourg and find that it not only fails but also lacks any potential to embrace data protection principles. These scholars have advanced three reasons to support their claims. First, there are comparatively few Strasbourg judgments that offer criteria for excessive, unnecessary, and/or unjustified collection of personal data.[25] According to them, this is due to the fact that the Court has overemphasized the legality requirement.[26] Second, based on these scholars' experience of this case law, they believe that many Court judgments allow processing authorities too much leeway.[27] Only flagrant abuse or risky use of data which is easily used in a discriminatory way is very closely scrutinized, whereas other kinds of processing of data are left untouched 'as long that there is no blood'.[28] Third, the very basis of data protection recognition in Strasbourg is not as solid as it looks.[29] For example, the ECtHR has on one occasion stipulated that Article 8 of ECHR does not give a general right to access personal data contrary to the data protection instruments.[30] Also, the Court has made a distinction between personal data that fall within the scope of Article 8 of the ECHR and personal data that do not.[31] De Hert and Gutwirth thus observe that in the eyes of the Court there is processing of personal data that affects the private life and processing of personal data that does not affect the private life of individuals contrary to the general protection of all personal data offered by data protection regulations.[32]

An overview of the above understandings attempting to distinguish *privacy* from *data protection* reveals three important conclusions. First, in a strict sense *privacy* and *data protection* are two distinct and separate concepts although they have overlapping objectives. The differences between the two concepts reside in their scope, goals, and content. However, it is important at this juncture to argue that those attempts which differentiate *privacy* from *data protection*—pointing out that the former is prohibitive while the latter is not—are illusive. For example, one of the mandatory legal preconditions for processing personal data in the Directive 95/46/EC is consent.[33] The notion of consent is traditionally linked to the idea that the data subject should be in control of the use that is being made of his data.[34] In turn the notion of control is linked to the fact that the data subject should be able to withdraw his consent consequently preventing any further processing of the individual's personal data by the data controller.[35] Also, consent is related to the concept of informational self-determination, making the autonomy of the data subject both a pre-condition and a consequence of consent.[36] In essence, consent gives the data subject influence over the processing of data.[37] However, although consent is one of the legal preconditions for processing personal data, it is not absolute. Sometimes the data subject's consent is difficult to obtain in real life[38] or it is subject to exemptions for the purposes of public interest such as defence and national security. Notwithstanding, it is arguable that consent is prohibitive to data processing activities, equating *data protection* to *privacy* to that extent. A similar view is maintained by De Hert and Gutwirth, although they generally view *privacy* as prohibitive as opposed to *data protection*. These scholars argue that data protection also prohibits certain forms of processing of personal data, for instance 'sensitive data'.[39] The second conclusion drawn from the attempts to differentiate *privacy* from *data protection* is that the two concepts are increasingly becoming synonymous and hence interchangeable in their daily uses. As rightly observed by Kuner:

> Calls for an international framework have tended to mix the terms 'data protection' and 'privacy'. For example, the resolution approved at the 30th International Conference in

24 Ibid, para. 118 of the Judgment.

25 De Hert and Gutwirth (n 4), at 23.

26 Ibid.

27 Ibid.

28 Ibid.

29 Ibid, at 24.

30 Ibid; see also *Gaskin v United Kingdom*, ECtHR, Strasburg, Application No. 10454/83 (1989), para. 37 of the judgment.

31 Ibid, at 24–5.

32 Ibid; see also *Pierre Herbecq and the Association Ligue des droits de l'homme v Belgium*. Cf. ECommHR, *Pierre Herbecq and the Association Ligue des droits de l'homme v Belgium*, Decision of 14 January 1998 on the applicability of Applications Nos 32200/96 and 32201/96 (joined) (1999) DRparas 92–98.

33 See, e.g., Art 7(a) and 8(2), (a) of the Directive 95/46/EC.

34 Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent', 01197/11/EN, WP187, p.8, (adopted 13 July 2011).

35 Ibid, at 9.

36 Ibid.

37 Ibid.

38 See, e.g., S. Elahi, 'Privacy and Consent in the Digital Era' (2009) 14/3 Information Security Technical Report 113–18, at 115; see also, EA Whitley, 'Informational Privacy, Consent and the "Control" of Personal Data' (2009) 14/3 Information Security Technical Report 154–9, at 155–6.

39 De Hert and Gutwirth (n 4), at 4.

> Strasburg quoted above [<http://privacyconference2008.org/index.php?page_id¼197>] refers to 'the rights to data protection and privacy', while the principles adopted by the 'Global Network Initiative', a group formed by a number of companies, non-governmental organizations, and academics, deal with 'the internationally recognized human rights of freedom of expression and privacy', thus focusing more on privacy than on data protection. The 'Global Privacy Standard', published in November 2006 by a working group led by Ontario Information and Privacy Commissioner, refers many times to 'privacy', but the principles themselves deal with topics such as consent, purpose limitation, and access rights, that have traditionally been thought to be key concepts of data protection law.[40]

The third conclusion is that when the context in which the concepts of *privacy* and *data protection* are used is not provided, one has to carefully scrutinize the principles covered, their scope and application. This is important because sometimes the true context in which these concepts are used needs to be identified in order to ascertain consequential implications from their application.

In this article both concepts: *privacy* and *data protection* are used interchangeably unless the specific context excludes the use of the other and any collective reference to *privacy and data protection* connotes either the former or latter term.

Methodology

The collection of literature reviewed in this article was gradual and has taken a long time. It actually started way back in 2005 when I was still a student of law at the University of Oslo, Norway, and continued until the time of writing the manuscript for this article. I used four main approaches to obtain such literature. The first method was through library membership: at the Norwegian Research Centre for Computers and Law (NRCCL), University of Oslo, Norway (2005–2006); Vrije Universiteit Brussels, Belgium (2009–date) where I am a freelance researcher with the Law Science Technology & Society (LSTS); Staats- und Universitätbibliothek Bremen, University of Bremen, Germany (2011–date); and University of South Africa (UNISA) (28 June 2011–29 June 2011). The second approach was through subscription to or purchase of relevant literature. Subscription to databases or the purchase of specific articles or issues containing such articles was mainly through the Internet. In some cases I purchased literature directly from bookstores. The third method I used is open source resources, for example, the Social Science Research Network (SSRN); African Journals Online (AJOL); Scandinavian Studies in Law Databases (Sc.St.L). It is worth mentioning that some of these resources are partly limited; I relied on permitted access. The fourth and final method involved making requests to authors of relevant literature to supply their works that I needed. Apart from that, this method served another important role. It facilitated my contact with data privacy experts across Africa, Australia, Europe, and America.

Literature review

The literature reviewed in this article consists mainly of published and unpublished works. In the former case, the survey is limited to books and published journal articles while the latter ranges from dissertations, conference and workshop paper presentations, commentaries, reports, and working papers. This literature extends from before 2005 to February 2012. Another factor limiting the scope of this review is language. Only literature published in English is reviewed. This is due to the linguistic limitation I had in accessing literature in other languages. Yet, it serves to communicate the issues I intend, as in most cases speakers of French or other languages possess some minimum understanding of English but the opposite is often not the case. Moreover, in order to facilitate and ease understanding of this literature, I have classified it by means of two criteria. The first is the geographical scope covered regardless of the originality of the author. Under this classification there is literature addressing issues covering Africa generally; West Africa; North Africa; Eastern Africa; Horn of Africa; and Southern Africa. Specific countries within particular regions may be indicated in the course of the review. This classification serves a number of purposes. It can roughly indicate which region and country has what level of literature. This in turn may explain the factors for the varying development of the literature on privacy and data protection in Africa. The second criterion for the classification of the literature in this article is based on specific themes addressed by a class of literature. This is important as it helps to avoid unnecessary repetition of common issues and themes addressed in the literature. Also significant, the classification offers a comparison of similar issues in different regions. Combining the two criteria, the present review will appear under subthemes and corresponding geographical region. I have

40 Kuner (n 9).

to mention one caveat. Sometimes one item of the literature may address issues transcending more than one region or theme. Yet no confusion is likely to arise as each piece will be treated as such in a specific region or sub-theme.

Concepts and theories of privacy in Africa

There is little literature that has dealt with the conceptualization of privacy in the African cultural context. So far Johann Neethling appears to be the only author who has attempted a definition of privacy in Africa.[41] However, Neethling's concept of privacy largely follows the pattern of Western theories of privacy, particularly in terms of control theory. On the other hand, Iain Currie has dealt with the concept of privacy based on the South African Constitution.[42]

Policies and data privacy regulations

Literature falling under this theme addresses, either generally or specifically, the status of policies and data privacy legislation in Africa. In 1999 David Banisar noted that no country in Africa had data privacy legislation.[43] Nevertheless he still noted that South Africa was reviewing the Open Democracy Bill. At the same time Banisar noted that by then Uganda and Namibia were considering in their parliaments the freedom of access of information Acts. In 2002 Serge Gutwirth took a similar view.[44] However, Gutwirth went further to point out that even the African Charter on Human and Peoples' Rights 1981 (ACHR) fails to mention privacy.[45] Moreover, he took cognizance of the fact that many African states mention privacy in their constitutions.[46] Yet such provisions have no significant impact in securing such right.[47] In 2004 Lee A. Bygrave pointed out, just like his predecessors, that none of the African countries had enacted comprehensive data privacy laws.[48] Like Banisar but differing slightly from Gutwirth, Bygrave noted that only South Africa had a constitution with a clause securing privacy and Kenya was drafting a new constitution based on the South African constitution.[49] Yet as did Gutwirth, he noted that ACHR omits to mention privacy.[50] Bygrave's views on the state of privacy are nearly wholly repeated by Elizabeth M. Bakibinga partly because she was influenced by the former's article published in 2004 and possibly because she is a former student of Bygrave.[51] In 2009 Adam Mambi listed South Africa, Mauritius, and the Seychelles as African countries with comprehensive data privacy legislation.[52] However, it is noteworthy that in 2010 by way of updating his previous work, Bygrave mentioned that four countries in Africa, chiefly Francophone, had adopted comprehensive data privacy legislation. The list includes Burkina Faso, Tunisia, Morocco, and Mauritius.[53] Interestingly, in the same year Kuner expanded this list to include two more countries with data privacy: Benin and South Africa.[54] Yet in the same publication, Kuner lists South Africa as being in the process of enacting data privacy legislation.[55] In 2011, in a global world map, Banisar listed Angola, Tunisia, Morocco, Senegal, Benin, and Burkina Faso as African countries with comprehensive data privacy legislation by 1 November 2011.[56] Perhaps a fairly comprehensive list of African countries with data privacy legislation is provided by Graham Greenleaf.[57] According to Greenleaf the list as it stood on 30 July 2011 includes Angola, Benin, Burkina Faso, Cape Verde, Mauritius, Morocco, Senegal, and Tunisia. In 2012, Greenleaf added the Seychelles to the list.[58] Moreover, Greenleaf's compilation lists the following African countries with

41 J Neethling, 'The Concept of Privacy in South African Law' (2005) 122/1 The South African Law Journal 18–28.

42 I Currie, 'The Concept of Privacy in the South African Constitution: Reprise' (2008) 2008/3 Journal of South African Law 549–57.

43 D Banisar, 'Privacy and Data Protection Around the World', Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999, 1–5, at 4, <http://www.pcpd.org.hk/english/infocentre/conference.html> accessed 26 February 2012.

44 S Gutwirth, *Privacy and the Information Age* (Rowman & Littlefield Publ.,Lanham/Boulder/New York/Oxford/ 2002).

45 Ibid, at 24.

46 Ibid, at 24–5.

47 Ibid.

48 Bygrave (n 16), at 343.

49 Ibid.

50 Ibid.

51 EM Bakibinga, 'Managing Electronic Privacy in the Telecommunications Sub-Sector: The Ugandan Perspective' (2004) <http//:thepublicvoic.org/eventscapetown04/bakibinga.doc> accessed 27 May 2012, at 4 and 9.

52 A Mambi, 'Internet Governance (IGF): Legal Issues on Cyber Security' Mauritius, March 2009 (PowerPoint presentation) 19, <http://www.atu-uat.org/images/presentations/IGF,MRTS,_CYBERSECURITY2,MAMBI.pdf> accessed 25 February 2012.

53 LA Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) 56 Scandinavian Studies in Law 165–200, at 193.

54 C Kuner, '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 <http://ssrn.com/abstract=1689483> accessed 26 February 2012.

55 Ibid, at 22 and 90.

56 D Banisar, 'Data Protection Laws around the World Map' <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416> accessed 26 February 2012.

57 G Greenleaf, 'Global Data Privacy Laws: Forty Years of Acceleration' (2011) 112 Privacy Laws & Business International Report 11–17 at 14–16.

58 G Greenleaf, 'Global Data Privacy Laws: 89 Countries, and Accelerating' (2012) 115 Privacy Laws & Business International Report, Special Supplement; also appears cited as Queen Mary University of London,

Bills and draft Bills on data privacy legislation: Ghana, South Africa, Madagascar, Mali, Niger, and Kenya. Information Shield provides that Morocco and South Africa are African countries with comprehensive data protection legislation.[59] Jeff Rohlmeir lists none of African countries as having data protection legislation.[60]

Apart from the general approach, some literature has focused on and provided the status of policies and data privacy law only in a particular country or some specific countries or sub-region. There is a handful of such literature. In South Africa, the majority of the literature cites that privacy is largely protected under the constitution and common law. In addition, this literature quite generally lists some sector specific legislation, mainly in the electronic communication sector, as securing privacy. It also discusses the pending Protection of Personal Information Bill 9/2009. The work of the following authors specifically serves as an illustration of the major literature on data privacy in South Africa: Johann Neethling *et al.*,[61] Anneliese Roos,[62] Ian Currie,[63] Iain Currie and Jonathan Klaaren,[64] Kate Allan and Iain Currie,[65] Jonathan Burchell,[66] Caroline Ncube,[67] and Hendrik Johannes Gerhardus Oberholzer.[68] In Mauritius there is currently one known publication in the form of an article authored by Claire Gayrel.[69] The latter briefly analyses the Data Protection Act 2004 in Mauritius. It is noteworthy that Gayrel's article is a direct product of a report analysing the adequacy of the Mauritian data privacy legislation by the European Union—a report for which Gayrel was among the consultants and authors.[70] In Zimbabwe, Caroline Ncube points that the country does not have comprehensive data privacy legislation.[71] Neither does its Constitution contain a privacy provision. Nevertheless, she contends that privacy can be read in other provisions of the Constitution, notably protection against arbitrary search or entry; protection against the reprivatization of property; and protection of freedom of expression. In addition, privacy is protected under the common law. The recently published article in Angola by João Luís Traça and Bernardo Embry[72] completes the review in the Southern Africa region. This article is the earliest comment on the data privacy legislation in Angola adopted in June 2011, before it was even put into implementation.

In Eastern Africa there is thin literature on the status of policies and data privacy legislation. John Ubena has

School of Law Legal Studies Research Paper No. 98/2012, pp. 1–13 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034> accessed 26 February 2012.

59 Information Shield., 'Information Privacy Law by Country' <http://www.informationshield.com/intprivacylaws.html> accessed 26 February 2012.

60 J Rohlmeir, 'International Data Protection Legislation Matrix' <http://www.accinfosys.com/docs/International_Data_Protection_Laws.pdf> accessed 25 February 2012.

61 J Neethling *et al.*, Neethling–Potgieter–Vesser Law of Delict (6th edn, LexisNexis, Durban 2010); J Neethling *et al.*, Neethling's Law of Personality (2nd edn, LexisNexis, Durban 2004).

62 A Roos, 'Data Protection for South Africa: Expectations Created by Open Democracy Bill, 1998', Proceedings of the Constitutional Right of Access to Information Conference, 4 September 2000, St George's Hotel, Rietvlei Dam, Pretoria, pp. 41–53; A Roos, 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study', LL.D Thesis, University of South Africa (UNISA) (2003); A Roos, 'Core Principles of Data Protection Law' (2006) 39/1 Comparative and International Law Journal of Southern Africa 103–30; A Roos, 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124/2 South African Law Journal 400–37; A Roos, 'Personal Data Protection in New Zealand: Lessons for South Africa?' [2008] PER 22, <http://www.saflii.org/za/journals/PER/2008/22.html> accessed 26 February 2012; A Roos, 'Data Protection' in M Dana, *et al*, Information and Communications Technology Law (LexisNexis, Durban 2008).

63 I Currie, 'Privacy and Forgetting: The Case of the TRC Archive', PowerPoint Presentation in the 25th International Conference of Data Protection and Privacy Commissioners, 11 September 2003, Sydney (Australia) <http://www.privacyconference2003.org/program.asp> accessed 26 February 2012; I Currie, 'The Protection of Personal Information Act and its Impact on Freedom of Information' (University of the Witwatersrand, Johannesburg, 2010) 1–9 <http://www.opendemocracy.org.za/wp-content/uploads/2010/10/The-Protection-of-Personal-Information-Act-and-its-Impact-on-Freedom-of-Information-by-Iain-Currie.pdf>, accessed 26 February 2012.

64 I Currie and J Klaaren, *Commentary on the Promotion of Access to Information Act* (*Siber* Ink, South Africa 2002); I Currie and J Klaaren, 'Evaluating the Information Bills: A Briefing Paper on the Protection of Information Bill', paper prepared on behalf of the Centre of Memory at the Nelson Mandela Foundation, 17 June 2011, <http://mg.co.za/uploads/2011/06/28/110617-currie-klaaren-evaluating-the-information-bills-548.pdf> accessed 26 February 2012.

65 A Kate and I Currie, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Regulator for South Africa, Current Developments' (2007) 23/3 South African Journal of Human Rights: Sexuality and the Law 570–86; also accessible at <http://www.wits.ac.za/files/res4cdd5f670f1f4175a03dd36f6b8a9985.pdf> accessed 26 Februaryy 2012.

66 J Burchell, 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13/1 Electronic Journal of Comparative Law 1–26, at <http://www.ejcl.org/131/art131-2.pdf> accessed 26 February 2012.

67 C Ncube, 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems' (2004) 2 Journal of Information, Law and Technology (JILT) <http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/ncube/> accessed 25 February 2012; CB Ncube, 'Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa' (2006) 3/4 SCRIPTed 344–54.

68 HJG Oberholzer, 'A Privacy Protection Model to Support Personal Privacy in Relational Databases', Msc. Dissertation, Rand Afrikaans University (2001).

69 C Gayrel, 'Mauritius: Data Protection in an Evolving Island Economy' (2011) 114 Privacy Laws & Business International Report 20–2.

70 C Gayrel *et al.*, 'Analysis of the Adequacy of Protection of Personal Data provided in Mauritius: Draft Final Report, 2010', Research Centre on IT and Law, University of Namur(Belgium) <http://www.fundp.ac.be/recherche/publications/page_view/70740/> (note that this report is not readily accessible).

71 Ncube (n 67).

72 JL Traca and B Embry, 'The Angolan Data Protection Act: First Impressions' (2012) 2/1 International Data Privacy Law 40–5.

recently published an article 'Privacy: A Forgotten Right in Tanzania'.[73] He notes that Tanzania has no data privacy legislation. Nevertheless, privacy is protected in a number of statutes such as the Human DNA Regulation Act 2009. In Uganda, Bakibinga reveals that the country has no data privacy legislation although privacy right is stipulated in the Ugandan Constitution 1995 and other statutory laws albeit in an *ad hoc* fashion.[74] In the same vein Kato Mivule and Claude Tuner posit, 'there is little or no known literature on data privacy from Uganda and much of sub-Saharan Africa in general, given the relatively young and developing computing domain. At this time, to the best of our knowledge, we are the first to call for the application of data privacy techniques in Uganda'.[75] A similar situation is seen in Kenya where Michael Murungi notes that no data privacy legislation exists.[76] Yet he points out that the protection of privacy is afforded in some statutes. Also, Murungi tells us that Kenya is currently considering a draft Bill (Draft Data Protection Bill 2009) on data privacy law. Article 19 [an organization that campaigns against laws and practices infringing basic human rights] had made its comments on this Bill to the effect that the proposed Bill is critically limited.[77] In particular, Article 19 raised concerns over the scope of the proposed law, which is restricted to the public sector while the private sector is left unregulated. Also, the draft Bill fails to exempt public servants from its application when they are conducting public business. The other issue raised by Article 19 is limited funding for the office of Information Commission that is charged with the implementation of the law. Finally, Article 19 is concerned with the use of unlinked concepts in the draft Bill, that is some concepts are provided in the definitions but are not mentioned again in the draft Bill. Iain Walden has generally considered the level of data privacy protection in the East African Community (Tanzania, Kenya, Uganda, Burundi, and Rwanda).[78] This is possibly the single known comparative study of data privacy policies and legislation in the Eastern Africa. Walden notes that there is no privacy legislation in any of the East Africa Community member countries.[79] Yet he notes further that only Rwanda and Kenya had issued proposals that address data protection and privacy issues. Also, Walden mentions that Rwanda has provisions in its Penal Code that criminalize infractions against privacy.[80] To a limited extent, Greenleaf has recently considered the state of privacy policies and law in the East African Community (EAC).[81] He notes that although there is a desire and some effort to enact such laws, currently only Kenya is the only country in the region considering draft legislation on data privacy law.

Little literature on the status of privacy is known to exist in the Horn of Africa. However, Alebachew B. Enyew's recent master of law thesis provides some useful guidance on the state of data privacy policy and law in Ethiopia.[82] Enyew reveals that in Ethiopia a privacy right is secured under the Ethiopian Constitution.[83] However, as of now, Ethiopia does not have data privacy legislation. Privacy protection can be found in scattered privacy provisions in the Criminal Procedure Code, Civil Code, and Freedom of Mass Media & Access to Information Proclamation.[84] Enyew generally finds the system of privacy protection in Ethiopia to be inadequate.

In North Africa, there is a recently published journal article by Claire Gayrel.[85] The article focuses on Tunisia and Morocco. As was the case with Mauritius, Gayrel relied on the adequacy assessment reports by the European Union, for which she was a member of the team of consultants for the assessment and also one of the authors of the report.[86] Essentially in her 2012 journal article on Tunisia and Morocco, Gayrel advances a comparison of the regime of data privacy in the two jurisdictions. She notes that while both countries have

73 J Ubena, 'Privacy: A Forgotten Right in Tanzania' (2012) 1/2 The Tanzania Lawyer 72–114.

74 Bakibinga (n 51).

75 K Mivule and C Turner, 'Applying Data Privacy Techniques on Tabular Data in Uganda' <http://arxiv.org/ftp/arxiv/papers/1107/1107.3784.pdf> accessed 26 February 2012.

76 MM Murungi, *Cyber Law in Kenya* (Kluwer Law International The Hague 2011) chs 6 and 8.

77 Article 19, 'Draft Data Protection Bill Critically Limited', Comments submitted to the Constitution Commission of Kenya (CCK) in October 2011 <http://www.article19.org/resources.php/resource/2825/en/kenya:-draft-data-protection-bill-critically-limited> accessed 26 February 2012.

78 I Walden, 'East African Community Task Force on Cyber Laws: Comparative Review and Draft Legal Framework', Draft v.1.0, 2/5/08 prepared on behalf of UNCTAD and the EAC, May 2008.

79 Ibid, at 8.

80 Ibid, at 8.

81 Greenleaf (n 58).

82 AB Enyew, 'Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia', LL.M Thesis, University of Oslo, Norway (20090.

83 Ibid, at 27–43.

84 Ibid.

85 C Gayrel, 'Data Protection in the Arab Spring:Tunisia and Morocco' (2012) 115 Privacy Laws & Business International Report 18–20.

86 See, e.g., C Gayrel *et al.*, 'Analysis of the Adequacy of Protection of Personal Data Provided in Tunisia: Final Report, 2010', Research Centre on IT and Law, University of Namur (Belgium) <http://alexandrie.droit.fundp.ac.be/GEIDEFile/6544.pdf?Archive=192619191089&File=6544_pdf> accessed 26 February 2012 (note that unlike the report on Mauritius, this report is readily accessible).

data privacy legislation, Morocco's law is closer to the European model (Directive 95/46/EC) while Tunisia's law, although modelled along the lines of the European law, falls significantly short of such a standard.

In West Africa, the literature on privacy and data protection policies and legislation largely focuses on the Economic Community of West African States (ECOWAS)[87] and individual countries in the region. The literature on ECOWAS largely presents in a glorious manner that, unlike other sub-regions of Africa, West Africa has comprehensive framework legislation at the sub-regional level (ie ECOWAS). This body of literature includes that authored by Graham Greenleaf,[88] Wale S. Ajala,[89] and Teki Akuetteh.[90] At the country level, Enyinna S. Nwauche writes on the state of privacy rights in Nigeria.[91] Nwauche contends that privacy in Nigeria is protected via the Nigerian Constitution 1999 and through the tort of breach of confidence or the tort of privacy. Yet he finds no decided case on the tort of breach of confidence in Nigeria. João Luís and Bernardo Embry write on the state of privacy and data protection in Cape Verde.[92] They note that in Cape Verde privacy is first of all protected under the Cape Verdean Constitution(2010 Revised Edition) as a correspondence of the communication right in Article 44 and as *habeas data* in Article 46. Over and above this, Cape Verde has had data privacy legislation since 2001 making her the first African country to enact such a law. Yet up to 2011(when Traça and Embry's article was published) Cape Verde had not yet established a data protection authority that would set the law in motion.

Culture and privacy

Literature on culture and privacy occupies the dominant discourse in explaining the state of privacy in Africa in this section. The main thrust of this literature is that privacy in Africa is undeveloped because of the prevalence of the culture of collectivism as opposed to the Western culture of individualism. Accordingly, the authors argue that as Africans live in associations, an individual is denied a space for claiming his/her right to privacy. To put this another way, what the authors of the literature on culture and privacy are arguing, is that individualism is a pre-condition for the existence of attitudes and values realting to privacy. Included in this strand of thought are scholars such as Gutwirth,[93] Bygrave,[94] Bakibinga,[95] Burchell,[96] and Olinger *et al.*[97] However, there are some important variations in this literature that it is worthwhile mentioning. For example, in 2004 Bygrave cautioned that African cultures should not be considered static categories.[98] He also pointed out that the provision for privacy rights is increasingly on the legislative agendas of some African countries. As to why there is this growing interest, Bygrave advances three main reasons: the obligation imposed by the International Covenant on Civil and Political Rights 1966; a desire to meet the adequacy requirements of Articles 25–26 of the EU Directive; and in some cases stimulus is provided by recent first-hand experience of mass oppression (eg South Africa).[99] Yet in 2010, in taking cognizance of the adoption of data privacy legislation by certain African jurisdictions, Bygrave offered a new explanation: this development partly reflects the efforts by the French data protection authority(Commission de l'Informatique et des Libertés (CNIL)) to cultivate data protection in former French colonies, but it also reflects economic concerns, particularly the desire by some of these countries to safeguard their outsourcing industry(this is the case with, eg, Tunisia and Morocco).[100] Bakibinga draws the interesting conclusion that one can have privacy and still be part of the community'.[101]

Olinger *et al.*'s observations and conclusions are equally worthy of being highlighted. Unlike the other scholars in this category, Olinger *et al.*, wrote specifical-

87 ECOWAS has 15 members: Benin, Burkina Faso, Cape Verde, Ivory Coast, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra-Leone, and Togo.

88 Greenleaf (n 58).

89 WS Ajala, 'Enabling Harmonisation of Cyber Legislation at the Sub Regional Level: Opportunities and Challenges', The Second Session of the Committee on Development, Information, Science and Technology (CODIST II) 2–5 May 2011, Addis Ababa, Ethiopia <http://repository.uneca.org/codist/sites/default/files/codist/ICT/Day1_May02/Enabling%20Harmonization%20of%20Cyber%20Legislation%20at%20the%20Sub%20Regional%20Level.pdf> accessed 26 February 2012.

90 T Akuetteh, 'Creating the Enabling Environment within ECOWAS Region', PowerPoint presentation <http://meeting.afrinic.net/waigf/presentations/Presentation_%20Ecowas_Teki_Akuetteh/Presentation_Ecowas_Teki_Akuetteh.pdf> accessed 26 February 2012.

91 ES Nwauche, 'The Right to Privacy in Nigeria' (2007) 1/1 Review of Nigerian Law and Practice 62–90.

92 JL Traca and B Embry, 'An Overview of the Legal Regime for Data Protection in Cape Verde' (2011) 1/4 International Data Privacy Law 249–55.

93 Gutwirth (n 44) at 24–5.

94 Bygrave (n 16) at 328; Bygrave (n 53) at 175–6.

95 Bakibinga (n 51) at 2, 4–5.

96 Burchell (n 66) at 2.

97 HN Olinger, *et al.*, 'Western privacy and/or *Ubuntu*? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa' (2007) 39/1 International Information & Library Review 31–43, at 35–6.

98 Bygrave (n 94) at 328.

99 Ibid, at 343.

100 Bygrave (n 53) at 194.

101 EPIC Alert, 'EPIC Hosts Privacy and Public Voice Conference in Africa' (23 December 2005) 11/24 EPIC Alert <http://www.epic.org/alert/EPIC_Alert_11.24.html> accessed 26 February 2012.

ly in response to comments on the South African Bill on data privacy. They examined whether the African collectivist culture manifesting itself in the name of *Ubuntu* in South Africa would have any impact on the proposed law. The authors' observations and conclusions can be summarized as follows. The influence of *Ubuntu* would be of less significance in the development of privacy legislation in South Africa.[102] These authors advance three main reasons for their view: first, although human dignity is the prime *Ubuntu* value that has been infused into the Constitution of South Africa there exist no *Ubuntu*-specific references to privacy in the Constitution in the current privacy related legislation in South Africa.[103] Second, although *Ubuntu* can, and indeed has, influenced jurisprudence in South Africa, it could only do so in those areas where *Ubuntu* has a strong expression and philosophy. In the case of privacy, *Ubuntu* leaves little doubt that privacy is not esteemed as priority for the community or for the individual.[104] Third, the notion of *Ubuntu* is to a certain extent an idealistic concept in a world of economic realities that is regulated and controlled by international standards, rules, and regulations such as those designed by, amongst others, the World Intellectual Property Organisation (WIPO) and the EU.[105] Because of that, *Ubuntu* is exclusive and limited to the African way of life. It is not incorporated into global trade agreements and its very nature is cultural, not legal or economical. On their finding of a great influence of the EU's data privacy law to the forthcoming data privacy law in South Africa, Olinger *et al.* advance three reasons. First, the protection of dignity which is a core expression of the EU's data privacy law overlaps with *Ubuntu*'s concept of human dignity, the South African Constitutional principle of dignity, as well as the common law concept of personal dignity.[106] Second, that the South African Constitution enshrines the right to privacy as a constitutional right, which is the highest possible order of protection and embodiment of a right.[107] This is similar to the description of the privacy right in the EU's privacy legislation which is comprehensive and also compulsory in all EU member states. Third, since the EU is the major trading partner of South Africa, its directives, charters, and protocols will have an influence and direct bearing on South Africa.[108] This is because of requirements under the EU's data privacy legislation which restrict the transfer of personal data to a third country unless it has adequate privacy protection.

Religion and privacy

Religion has also been studied in the context of privacy. In particular the literature in this area has tended to focus primarily on Islamic religion. The dominant discourse is that Islamic religion and practices produce an unfavourable environment for individuals to advance claims for individual privacy. Two things are frequently discussed as affecting privacy. First, the majority of jurisdictions with a Muslim population favour adopting Islam as the state religion. Second, but somewhat linked to the first, such states tend to adopt *sharia* law as the supreme law of the land, undermining any constitutional right to privacy and eroding the traditional roles of organs established by such constitutions. However this view has been resisted and favourable arguments that make Islam compatible with privacy have been advanced even where practices are inconsistent to these arguments. In the African context, the literature on Islam and privacy focuses on North Africa and the West African state of Nigeria, particularly the northern states which are predominantly Islamic. A joint article by Mireille M. Caurana and Joseph A. Cannataci[109] and a sole-authored article by Ayo Kusamotu[110] are important sources in this part of the review.

To begin with, Caurana and Cannataci examine the impact (applicability) of EU Directive 95/46 on the protection of personal data in the North Africa and Middle Eastern states where Islamic culture or Islamic law underlies much of everyday legal practice. According to the authors, this examination was prompted by one major factor: the movement by EU-based industries of more and more of their operations to North Africa and Islamic law states in order to take advantage of lower labour costs.[111] Focusing on Tunisia, the authors point out that Tunisia has adopted a law on

102 Olinger *et al*, (n 97) at 40.
103 Ibid.
104 Ibid.
105 Ibid.
106 Ibid, at 40–1.
107 Ibid, at 41.
108 Ibid.
109 MM Carauna and JA Cannataci, 'European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States' (2007) 16/2 Information & Communications Technology Law 99–124.
110 A Kusamotu, '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' (2007) 16/2 Information & Communications Technology Law 149–59.
111 Ibid, at 100.

data protection. However, they argue that although such a law is *prima facie* word perfect *vis-à-vis* EU Directive 95/46, its implementation is possibly seriously marred by, among other things, the use of personal data for police purposes, which reportedly falls far short of the EU standard entrenched in Recommendation R(87)15.[112] Kusamotu considers the Nigerian legal framework for the protection of privacy in the context of the 'adequacy' test in EU Directive 95/46/EC. His analyses reveal that such a legal framework fails to meet the standard set by the European law. Kusamotu raises three important points: first, Nigeria does not have specific privacy laws, but guarantees the right to privacy in her Constitution; second, Article 37 of the Nigerian Constitution 1999 on protection of the right to privacy is discriminatory and segregative to non-Nigerians. This provision states 'the privacy of citizen . . . ' Accordingly Kusamotu argues, 'it would therefore appear that in the case of the personal data of non-Nigerians that are being processed or are to undergo processing after being transferred to Nigeria, the individuals concerned will not be able to enforce their fundamental right to privacy under the Constitution';[113] third, that the absence of data protection laws in Nigeria is not connected to the percentage of Muslims in Nigeria's population or to any tenet of faith, Muslim, Christian, or otherwise, but rather to the low level of data processing and awareness about its implications for privacy.[114]

Developmentalism and privacy

The literature surrounding development and privacy tends to argue that the current diminishing state of privacy in Africa is a result of developmentalism efforts by African countries after independence. According to the authorities in this strand, African countries neglected to deal with privacy issues as were of no priorities to the countries. Ncube is the leading scholar to maintain this view.[115] She argues, 'from the time of independence Zimbabweans have been predominantly concerned with those rights pertaining to pressing political and economic issues such as the rising cost of living. Subsequently, issues such as data protection have been largely overlooked.'[116]

ICTs and privacy

Literature under this heading treats the penetration and use of information and communication technologies (ICTs) in Africa as among the catalysts for the rising concern for privacy. Usually the massive collection of personal information and the relatively easy possibilities for abuse of such information have generated public fears about individuals' privacy. Authorities who have clearly linked ICTs with the rise of privacy concerns in Africa include the following: Banisar,[117] Roos,[118] Bakibinga,[119] Kusamotu,[120] and Enyew.[121] Of these scholars, Banisar seems to have made a fairly detailed analysis of the threat posed by ICTs in the African contexts. He has dealt with information systems and privacy including developments of national ID card systems, biometric passports, DNA databases, and body scanners. He also dealt with communications issues such as surveillance capabilities, identity of users, and cyber-crimes. Other scholars who have fairly dealt with issues of ICTs and privacy include Human Rights Watch,[122] Alex Comninos,[123] and Ilhem Allagui.[124] The latter two authorities have dealt with the role of ICTs in the context of the Arab spring in Tunisia, Egypt, and Libya. Their literature shows to what extent ICTs, particularly social networks (Twitter and Facebook), were used by the protestors to organize and wage protests and at the same time to what extent and how the regimes in those countries relied on the same or facilities to snoop on protestors.

Telecommunication and privacy

This literature is somewhat related to that in the previous paragraph, but it was not discussed there because of its specialized nature. There is a large body of literature developed under this theme. However, a few points must be made clear. First, the literature on telecommunications (including other forms of electronic communication) has mushroomed partly because of

112 Carauna and Cannataci (n 109) at 115.

113 Kusamotu (n 110) at 154.

114 Ibid, at 157.

115 Ncube (A Comparative Analysis of Zimbabwean and South African Data Protection Systems) (n 65).

116 Ibid.

117 D Banisar, 'Linking ICTs, The Right to Privacy, Freedom of Expression and Access to Information' (20100 16/1 East African Journal of Peace & Human Rights 124–54.

118 Roos (n 62).

119 Bakibinga (n 51).

120 Kusamotu (n 110).

121 Enyew (n 82).

122 Human Right Watch., 'The Internet in Mideast and North Africa: Free Expression and Censorship', Human Rights Watch 1999 <http://www.hrw.org/sites/default/files/reports/midintnt996.PDF> accessed 26 February 2012.

123 A Comninos, 'Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond', Association for Progressive Communications (APC) (June 2011), 1–18, at 5 <http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf> accessed 26 February 2012.

124 I Allagui, 'The Arab Spring and the Role of ICTs: Editorial Introduction' (2011) 5 International Journal of Communication 1435–42.

two factors: first a recent requirement for the mandatory registration of SIM cards in many African countries. Included in the list of countries with mandatory SIM card registration are Tanzania, Kenya, Nigeria, Botswana, Ghana, Mozambique, South Africa, Zimbabwe, Burundi, Rwanda, Gambia, Sierra Leone, Liberia, Algeria, Cameroon, Cote d'Ivoire(Ivory Coast), and Uganda. The literature has partly followed this pattern. Second, the recent adoption of interception of communication laws in some African jurisdictions. Authorities writing on this theme include Roos,[125] Ewan Sutherland,[126] Ncube,[127] Tracy Cohen,[128] Dumisani Ndlela,[129] Jacob Mapfume,[130] Alex B. Makulilo,[131] Michael Murungi,[132] Stephen C. Kaduuli,[133] Ronald K. Mayambala,[134] Bakibinga,[135] Amnesty International,[136] Chikaodili J. Hemeson,[137] Kajo Anan,[138] Chukwuyere E. Izuogu,[139] Iheanyi S. Nwanko,[140] and Franklin F. Akinsuyi.[141] The issues considered by these scholars are similar. They include the mandatory registration of SIM cards without an enabling law in place; secret interception of communications; poor database security; poor verification of consumers' information during registration; the authorization of interception; a lack of an effective enforcement system; and inadequate remedy or lack of a remedy at all when infringement occurs.

Health and privacy

The literature on health and privacy has largely been manifested in the context of HIV/Aids. This is partly because Africa is by far the continent most affected by the HIV pandemic. Reports reveal that by the end of 2010 an estimated 22.9 million people were living with HIV in sub-Saharan Africa, a figure which was equal to 68 per cent of the world population living with HIV at that time.[142] The pandemic had cost the lives of 1.3 million people in the sub-continent by 2009 leaving 1.8 million newly infected.[143] Efforts to prevent or provide care and support to people living with HIV/Aids have raised a number of privacy law issues. Consent to HIV/Aids testing is the most controversial issue surrounding privacy. Many people in Africa are concerned about HIV/Aids testing without their consent. Since HIV/Aids has no cure, many people consider their health

125 Roos (Data Protection) (n 62).

126 E Sutherland, 'The Mandatory Registration of SIM Cards' (2010) 16/3 Computer and Telecommunications Law Review 61–3.

127 Ncube (Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa) (n 67).

128 T Cohen, '"But for the Nicety of Knocking and Requesting a Right of Entry": Surveillance Law and Privacy Rights in South Africa' (2001) 1/1 The Southern Africa Journal of Information and Communication <http://link.wits.ac.za/journal/j-01-tc.htm> accessed 26 February 2012.

129 D Ndlela, 'Interception of Communication Act: The Fear of a Zimbabwean' <http://www.bizcommunity.com/Article/238/15/17757.html> accessed 26 February 2012.

130 J Mapfume, 'Analysis of the Interception of Communication Bill 2006: Interception and Deception!', Paper written for Media Institute of Southern Africa-Zimbabwe Chapter, 21 April 2006 <http://www.docstoc.com/docs/52158774/Analysis-of-the-Interception-of-Communication-Bill-2006-Interception> accessed 26 February 2012.

131 AB Makulilo, 'Registration of SIM Cards in Tanzania: A Critical Evaluation of the Electronic and Postal Communications Act 2010' (2011) 17/2 Computer and Telecommunications Law Review (CTLR) 48–54.

132 M Murungi, 'Registration of Mobile Phone Users: Easier said but carefully done' (26 July 2009) Kenya Law <http://kenyalaw.blogspot.com/2009/07/registration-of-mobile-phone-users.html> accessed 26 February 2012.

133 SC Kaduuli, 'To Tap or Not to Tap? This is the Uganda Phone Question' in Jilla Ramakistaisah (ed.), *Wiretapping: Regulatory Perspectives* (Icfai University Press, Hyderabad, India 2010) 209–19, at SSRN <http://ssrn.com/abstract=993545> last visited 26 February 2012.

134 KR Mayambala, 'Phone-tapping and the Right to Privacy: A Comparison of the Right to Privacy in Communication in Uganda and Canada', British & Irish Law, Education and Technology Association (2008) <http://www.bileta.ac.uk/Document%20Library/1/Phone-> tapping% 20and% 20the% 20Right% 20to% 20Privacy% 20% 5BRonald% 20Kakungulu% 5D.pdf accessed 26 February 2012.

135 Bakibinga (n 51).

136 Amnesty International., 'Uganda: Amnesty International Concerns on the Regulation of Interception of Communications Bill, 2007' (Amnesty International Publications 2007) <http://www.amnesty.org/en/library/asset/AFR59/005/2008/en/10bf8327-7507-11dd-8e5e-43ea85d15a69/afr590052008en.pdf> accessed 22 February 2012; Amnesty International, 'Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act 2010' (Amnesty International Publications 2010) ; <http://www.amnesty.org/en/library/asset/AFR59/016/2010/en/4144d548-bd2a-4fed-b5c6-993138c7e496/afr590162010en.pdf> accessed 26 February 2012.

137 CJ Hemeson, 'Directive on Consumer Data for SIM card Registration in the Telecommunications Sector: An African Perspective' (2012) Social Science Research Network 1–12 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1982033> accesses 26 February 2012.

138 K Anan, 'What is My Beef Against SIM Card Registration in Ghana?, Independent Civil Advocacy Network, 25 January 2010 at< http://www.i-can-ghana.com/?p=104> accessed 26 February 2012.

139 CE Izuogu, 'Data Protection and Other Implications in the Ongoing SIM Card Registration Process' (2010) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665> accessed 26 February 2012; see also CE Izuogu, 'Nigeria: Data Protection & Privacy Issues in NCC's Directive on SIM Card Registration' (2010) <http://www.facebook.com/note.php?note_id=388277770826> accessed 26 February 2012.

140 IS Nwanko, '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 26 February 2012; IS Nwanko, 'Part II: Nigeria's SIM Card Registration Regulations 2010: The Implications of unguarded Personal Data Collection' <http://www.facebook.com/note.php?note_id=10150095718055827> accessed 26 February 2012.

141 FF Akinsuyi, '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 26 February 2012.

142 UNAIDS, 'World AIDS Day Report 2011' 7 <http://www.unaids.org/en/media/unaids/contentassets/documents/unaidspublication/2011/JC2216_WorldAIDSday_report_2011_en.pdf> accessed 26 February 2012.

143 UNAIDS, 'UNAIDS Report on the Global AIDS Epidemic' 20 <http://www.unaids.org/documents/20101123_GlobalReport_Chap2_em.pdf> accessed 26 February 2012.

records in the context of HIV/Aids as most sensitive, fearing stigmatization.[144] The second issue stemming from the first is about disclosure of HIV/Aids test results or status to third parties without the authorization of the people concerned. This has resulted in serious problems in the health and employment sectors. Medical practitioners in Africa claim to be in dilemma whether to disclose or not to disclose an HIV/Aids status to a victim's sex partner or relatives, as the case may be.[145] Yet in some cases, without any consent from a concerned person, they have secretly been communicating HIV/Aids test results directly to employers while bypassing the employees who were the subject of testing.[146] Somewhat linked with the second issue, is discrimination of people living with HIV/Aids. Once their HIV/Aids status is revealed, many people living with HIV/Aids have found themselves discriminated against. This discrimination does not just end with the employment sector as is commonly cited by commentators[147] but extends to other spheres of life. In Kenya, discrimination has also manifested in issues of land ownership.[148] Nevertheless in relative terms, concerns for privacy in the context of HIV/Aids in Africa has manifested through the development of a larger corpus of case law on privacy.[149]

E-Commerce and privacy

The literature on e-commerce and privacy is relatively lacking. Although, at the risk of generalizing, this is partly due to the fact that e-commerce in Africa is low compared to the rest of the world. There is across Africa an inadequate e-commerce infrastructure. However, in relative terms, South Africa is far more advanced in e-commence than any other African country.[150] Because of that, research in this area is still evolving. Some authorities known to have canvassed privacy in the context of e-commerce include: Philip Plückhahn,[151] Janie Joubert and Jean-Paul van Belle,[152] Anthony C. K. Kakooza[153] and the Department of Communications–Republic of South Africa.[154] It is also imperative to note, there is a paper by an unnamed author based on empirical research of websites supporting e-commerce in South Africa and issues of privacy.[155] Throughout the period of collection, efforts to obtain its author have been made in vain, yet the same is published on a credible website. For this reason this review has decided to include it. Issues addressed in these works relate to consumer trust and confidence; cyber-crimes; and identity thefts.

Analysis

The above review of literature reveals that the corpus of data protection scholarship is still in its nascent stage. This is unsurprising, partly due to the fact that privacy and data protection is a new field of law in Africa, with only a few experts having a research interest in the subject. Relatively, South Africa is far more advanced compared to the rest of African countries in terms of this literature. This is probably because privacy and

144 See, eg, SD Weiser *et al.*, 'Routine HIV Testing in Botswana: A Population-Based Study on Attitudes, Practices, and Human Rights Concens' (2006) 3/7 PLoS Medicine 1013–22, at 1018–19; NC Mbonu *et al.*, 'Stigma of People with HIV/AIDS in Sub-Saharan Africa: A Literature Review' (2009) Journal of Tropical Medicine, Article ID 145891, doi:10.1155/2009/145891; P Anglewicz and J Chintsanya, 'Disclosure of HIV Status between Spouses in Rural Malawi' (2011) 23/8 AIDS Care: Psychological and Socio-Medical Aspects of AIDS/HIV998–1005, at 1002; The Wold Bank, *Legal Aspects of HIV/AIDS: A Guide for Policy and Law Reform* (The World Bank, Washington, DC 2007) <http://siteresources.worldbank.org/INTHIVAIDS/Resources/375798-1103037153392/LegalAspectsOfHIVAIDS.pdf> acccessed 26 February 2012.

145 See, eg, L Vu *et al.*, 'Disclosure of HIV Status to Sex Partners Among HIV-Infected Men and Women in Cape Town, South Africa' (2012) 16/1 AIDS Behaviour 132–8.

146 AB Makulilo, 'You must take medical test: Do Employers intrude into Prospective Employees' Privacy?' (2010) 8 Datenschutz und Datensicherheit (DuD) 571–5.

147 See, eg, JA Dwasi, 'The Human Right to Work in the Era of HIV and AIDS' (2009) Law Africa, Nairobi/Dar es Salaam/Uganda; Makulilo (n 146).

148 M Aliber and C Walker, 'The Impact of HIV/AIDS on Land Rights: Perspectives from Kenya' (2006) 34/4 World Development 704–27.

149 For a detailed review of case law on HIV/Aids in African jurisdictions see eg, MT Ladan, 'The Role of Law in the HIV/AIDS Policy: Trend of Case Law in Nigeria and Other Jurisdictions', Inaugural Lecture delivered at the Ahmadu Bello University, Zaria, Nigeria, 2008, pp. 1–64, at 19–22; MA Tadesse, 'HIV Testing from an African Human Rights System Perspective: An Analysis of the Legal and Policy Framework of Botswana, Ethiopia and Uganda', LL.M Thesis, University of Pretoria, South Africa (2007).

150 See, eg, Ncube (Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa), (n 67), at 345, 346–7.

151 P Plückhahn, '(E-Commerce) Data Protection in the European Union and South Africa: A Comparative Study', Msc Thesis, Aarhus University (Denmark) (2010).

152 J Joubert and JP Belle, 'Compliance of South African E-commerce Websites with Legislation to Consumer Rights', Information Technology and Organisations in 21st Century <http://www.commerce.uct.ac.za/informationsystems/staff/personalpages/jvbelle/2009/IBIMA04%20-61%20Compliance%20Ecommerce%20Consumer%20Legislation.pdf> accessed 27 May 2012.

153 ACK Kakooza, 'Embracing E-commerce in Uganda: Prospects and Challenges' Uganda Christian University (2008) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1658659> accessed 26 February 2012.

154 Department of Communications–Republic of South Africa, 'A Green Paper on Electronic Commerce for South Africa', November 2000 <http://www.info.gov.za/view/DownloadFileAction?id=68917> accessed 26 February 2012.

155 (Unnamed author), 'Data Privacy and Consumer Protection in South African E-commerce', <http://freedownload.is/doc/data-privacy-and-consumer-protection-in-south-african-e-commerce-9540616.html> accessed 26 February 2012.

data protection form part of the curriculum in some universities and hence there is a growing number of experts with an interest in the subject. In the rest of Africa the situation is not satisfactory. With the exception of Tanzania which has ICT law teaching at master degree level currently only at the Open University of Tanzania (with the support of the International Telecommunication Union and experts from the University of Strathclyde in Scotland), and at least the University of Dar es Salaam, where ICT law is taught at undergraduate only as an optional subject(or as an elective for an advanced coursework paper at postgraduate level), little is known for similar institutions teaching ICT law in Africa. However, in mitigating this problem, experts from different African countries are trained abroad, especially in Europe and the United States. Since financing training abroad is quite expensive, the number of these experts is still relatively small.

The review has also discovered that there is a virtually total lack of comparative studies in Africa on privacy and data protection. Many publications focus on a specific jurisdiction, quite often the country of residence of the authors. However, there are exceptions. The little comparative literature available can be classified into two groups. One group engages comparison between an African jurisdiction and a foreign one (outside Africa). This is the case with some of Roos' works. Illustrations of other literature falling under this category are the works of Mayambala and Plückhahn. The other category of comparative literature involves African jurisdictions as demonstrated by one of the journal articles of Ncube (involving Zimbabwe and South Africa) and Gayrel (involving Tunisia and Morocco). This lack of comparative literature can be explained by a number of possible reasons: a lack of research funds; a lack of networking among experts; the limited accessibility to literature authored by other scholars in different jurisdictions; a limited knowledge of legal systems of other jurisdictions; limited skills in undertaking comparative studies; linguistic barriers; cultural barriers; political and security reasons; and so on. The complaint by the Ugandan authors Mivule and Tuner illustrates some of these problems. Their statement deserves to be rewritten: 'there is little or no known literature on data privacy from Uganda and much of sub-Saharan Africa in general, given the relatively young and developing computing domain. At this time, to the best of our knowledge, we are the first to call for the application of data privacy techniques in Uganda.'[156] The interesting part of this complaint is the self-declaration to be the first scholars to deal with issues of privacy in Uganda.

Somewhat linked to the issue of comparative literature is the growing tendency of a substantial amount of the material to turn into *pseudo comparative studies or literature*. The latter situation arises where an item of literature on a particular African jurisdiction maintains an unreasonable length of background information based on non-African foreign jurisdictions, particularly European and US law and materials, leaving only a few paragraphs for discussion of the African jurisdiction. Arguably most of this literature remains too descriptive of what is obvious or known rather than being analytical and at best it fails to contribute to the development of the emerging African scholarship on data privacy. Some examples of this literature warrant mention with brief analysis. However, for want of space, I will take one most recent illustration of a journal article by Ubena—'Privacy: A Forgotten Right in Tanzania'. The title of this article promises much about Tanzanian privacy rights. Yet, on reading it one finds European data privacy law dominating the stage. It is surprising in an article that has 42 pages (72–114), that reference to Tanzania is restricted to a total space of just four pages. One would have expected to find the anatomy of the entire system of privacy in Tanzania albeit without comprehensive data privacy legislation, how it operates in practice, the constraints on its operation, etc. In my view it is not sufficient to mention that Tanzania has no comprehensive data privacy legislation. Perhaps an explanation for that would have been useful. It appears Ubena wants his audience to believe that once a comprehensive data privacy law is adopted in Tanzania, privacy will be automatically secured. This is certainly misleading because even in Europe privacy is infringed in the face of comprehensive data privacy legislation.

Also important to note, the above literature contains some serious factual errors. This can be seen particularly in matters of the status of policies and data protection regulations discussed above. There are two sets of these errors. First, there is inclusion and exclusion of countries from a list of African jurisdictions with data privacy legislation. Sometimes it is difficult to understand the correct current list of countries with data privacy law in Africa. It can be seen, for example, that in 2010 Bygrave and Kuner maintain different lists. Likewise in 2002 and 2004 both Gutwirth and Bygrave maintained that no African jurisdiction had data privacy legislation. Interestingly in 2004 Bakibinga quoted Bygrave to say no African jurisdiction had com-

156 Mivule and Turner (n 75).

prehensive data privacy. In 2011 Greenleaf too made some omissions of jurisdictions in Africa with data privacy legislation. Yet in 2012 he updated this position to present the correct list. The second factual error, related to the first, is the chronological timing of the adoption of such laws. Greenleaf's 2012 list correctly provides the timing for the adoption of data privacy legislation in Africa. But what do these factual errors tell us? Surely the problem is one of the accessibility to reliable information and literature in the African context. I will turn to this shortly.

Moreover some of the literature contains contradictions in its analyses. The literature on culture and privacy serves as an illustration. The strand takes collectivist culture as its independent variable for the state of privacy in Africa. Yet subsequently, this scholarship abruptly departs from its original premise. For example in 2004 Bygrave suggested that although African countries had no data privacy legislation due to the culture of collectivism, he left open the possibility of the African countries and particularly their collectivist culture to change. This possibility is captured in his own words, 'African cultures should not be painted static categories'. By any standard of interpretation Bygrave was suggesting that in a particular stage of its development, African culture would turn into individualism, hence providing the optimum environment for privacy to take root in the region. However, contradictions to that view started in the same year (2004) when he went further to point out that the interest in legislating in Africa was also due to the impact of Articles 25 and 26 of EC Directive 95/46 and the desire by African countries to meet the requirements of European law set out in those provisions. Similarly Bygrave identified recent first-hand experience of mass oppression (eg South Africa) as the stimulus for the adoption of data privacy law. The question is, can these two factors operate in an environment where the culture of collectivism is prevalent? In 2010 Bygrave departed further by saying that the emergence of data privacy law in the former French colonies was a result of the efforts of the French data protection authority(Commission de l'Informatique et des Libertés (CNIL)) to cultivate data protection in former French colonies. Bygrave does not explain what he meant by 'cultivating data protection'. Moreover, he does not offer any detail as to how the data protection authority in France 'cultivated' data protection in the former French colonies. Where is our independent variable? Admittedly more than one factor can operate jointly to different degrees to produce one desired effect. But can the emergence of data privacy legislation in some African jurisdictions offer sufficient evidence of the African cultural transformation that was foreseen by Bygrave (ie from collectivism to individualism)? If not, how can such legislation be made to operate in an environment dominated by a collectivist culture? Or should it be argued that African countries are adopting data privacy merely to meet the criteria of Articles 25 and 26 of the European Directive?

Apart from such contradictions, some of the literature has misplaced the contexts of their analyses. It is sufficient to point out one example by Gayrel. In her latest article she has adopted the title 'Data Protection in the Arab Spring: Tunisia and Morocco'. Immediately I saw this title I linked its analyses to the Arab revolutions in Tunisia and Morocco. Unfortunately I was a victim of the saying 'don't judge a book by its cover'. The message conveyed by this article was different. It was comparing data privacy legislation in Tunisia and Morocco. Moreover, the article's analyses were triggered by reports and analysis of the adequacy of personal data protection in such countries carried in 2010, well before the Arab Spring. The author makes only one reference to the Arab Spring in a single sentence at the end of her article (p. 20). Since this is not fiction, the message needs to tally with its title however stylistically it is formulated. The way the title of Gayrel's article appears is misleading and may make her audience pick it readily while assembling a literature review only to find later that it has nothing to do at all with the Arab Spring.

The literature also depicts a growing interest by European scholarship in Africa. However, most of it has been offshore and *ad hoc* in nature and without detailed analyses of the African socioeconomic and political environment (see, eg, Bygrave, Gutwirth, Greenleaf). Perhaps a relatively more detailed literature is that authored by Gayrel. It is submitted that joint researches by European scholars with Africans may stimulate the development of data privacy in Africa. This is partly because of the limitations the former suffer in understanding African contexts.

As pointed out, limited accessibility to information is one such constraint which impedes research in Africa. This limitation may be due to different reasons: infrastructure (eg poor internet connectivity); lack of research funding; and a lack of networking and cooperation among researchers. I have to point out that the limitation to access of information does not necessarily come from within Africa. Sometimes it originates from outside. I will briefly explain, as I have myself suffered this ordeal. In December 2011, I made a request for a supply of four reports from researchers who undertook a study on the analysis of the adequacy of personal data protection in Mauritius, Tunisia, Burkina Faso,

and Senegal. I needed the reports as part of my ongoing research on data protection in Africa. Some of those researchers opted not to reply my request. However, one of them replied to my request telling me that the reports were confidential as the research study giving birth to such reports was commissioned by a client. I was advised to ask the client for the reports directly. While my request to the client is still pending to date, one of the researchers who opted not to reply to my request has up to now issued two publications in the form of journal articles based on three of the reports I requested. The question is, if those reports were confidential in the first place why has it occurred they are being extracted and made available to the public? Are these reports still confidential?

Conclusion

The overview of the above review of the literature on data privacy policies and regulations in Africa indicates that its current state is underdeveloped. Yet, there are prospects for continued growth. Such growth, however, depends on various factors. In this article I make a modest proposal that experts establish a network as a starting point. To start with, networking may be established from the level of two or more experts within and outside their countries. With time, many will come to know each other and exchange experiences. In the course of this networking, experts may come together in joint writing or by facilitating each other to gain access to information in foreign jurisdictions. From the stage of knowing each other, formal networks may be established through institutions or other possible avenues. Out of the formal networks, experts may plan and think of the best ways of moving forward, particularly in carrying out research that is relevant to solving the problems facing their countries.

doi:10.1093/idpl/ips014
Advance Access Publication 11 June 2012