



African Journal on Privacy & Data Protection

To cite: MA Simiyu 'Exploring the legal manoeuvres for an equilibrium between access to information and privacy rights in Kenya and South Africa' (2025) 2
African Journal on Privacy & Data Protection 61-82

Exploring the legal manoeuvres for an equilibrium between access to information and privacy rights in Kenya and South Africa

*Marystella A Simiyu**

Africa Senior Legal Advocacy Officer at the International Press Institute

Abstract

An enforcement tension between the right of access to information and privacy is inevitable insofar as the foundation of one right is information disclosure, the other being control of disclosure. Both rights, however, are not absolute in nature and are subject to reasonable and justifiable limitations, allowing the intervention of international, regional and national laws to reconcile competing interests. The balancing of these rights in African legal frameworks is of key interest in Africa where the value of the right to privacy has been contested. However, the evolution of legal instruments such as the African Union Convention on Cyber Security and Personal Data Protection and the African Commission Declaration of Principles on Freedom of Expression and Access to Information in Africa is reflective of the legal adaptation to the contemporary needs of African societies on privacy and information. These instruments together with the Guidelines on Access to Information and Elections in Africa confront the challenges faced with the realisation of both access to information and right to privacy and data

* LLB (Kenyatta University); LLM (Centre for Human Rights, University of Pretoria) & LLD (University of Pretoria) – mssimiyu@gmail.com

protection. This article focuses on the impact of this equilibrium in promoting good governance, transparency and accountability, including during elections, towards nurturing an informed and engaged electorate and public. In dissecting the domestication of the provisions in international and regional instruments, and national approaches to facilitating these rights, the article examines the legal systems in Kenya and South Africa. The article finds that a common anchoring consideration in balancing access to information and privacy rights is a public interest override that outweighs the envisioned harm.

Key words: access to information; privacy; data protection; elections; competing rights

1 Introduction

Paradoxically, the complete enjoyment of human rights rests on limiting the exercise of certain rights that may be in conflict.¹ The rights of access to information and privacy are in a potential collision in as much as they pursue opposing objectives of information disclosure and information control, respectively. However, both rights enjoy fundamental status under international law. The majority of national constitutions reconcile competing interests in rights by imposing limitations. Generally, rights limitations are guided by the principles of legality, legitimate aim, and necessity and proportionality in a democratic society.² Absolute rights are only marginally recognised under international law, revealing an expectation of conflicting rights.³

The growing corpus of international and national laws has attempted to address the conflict between the right to information and privacy rights. This is especially so in the wake of the implications of globalisation and digital technologies on the exercise of these rights and other rights, including the right to meaningful public and political participation. By employing the human rights approach, this article examines how frameworks at the United Nations (UN) and African levels as well as national legal systems in Kenya and South Africa have approached the reconciliation of these rights. This article is structured in five parts. Part 1 is this introduction. Part 2 unpacks the definition of privacy and its correlation with access to information. Part 3 analyses how the UN and African legal frameworks address the competing interests concerning access to information and privacy. This part zeros in on the substance and implementation of the Guidelines on Access to Information and Elections in Africa using practical examples from

1 A Bilgorajski 'Boundaries and limitations of human rights. A contribution to the discussion' (2023) 27 *Ain Shams Engineering Journal* 68.

2 General Comment 34, Article 19: Freedom of opinion and expression, CCPR/C/GC/34 paras 24-36, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf> (accessed 5 August 2024).

3 For examples of absolute rights, see art 7 and 8 of the International Covenant on Civil and Political Rights (ICCPR) on freedom from torture and slavery respectively, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (accessed 5 August 2024).

South Africa and Kenya. Part 4 examines how statutes and case law in Kenya and South Africa find the middle ground between privacy and access to information. Part 5 concludes the article.

2 The conceptual intersection between privacy and access to information

Conceptualising privacy has been the subject of considerable intellectual discourse.⁴ While there is no accepted consensus on the definition of privacy, the notion of ‘access’ features strongly in characterisations of the term ‘privacy’. Access in this sense is relational and may pertain to access to a person, be it a tangible physical state or intangible psychological state.⁵ In one of the early descriptions of privacy, Cooley writes of the right to be left alone.⁶ Scholars Warren and Brandeis further depict this right to be left alone or privacy right as a component of a more holistic and evolving portrayal of the right to life and the enjoyment of life.⁷ One’s desire to exercise control over their state of solitude, anonymity and secrecy, key aspects of privacy, features strongly in this definition.⁸ Gerety, similarly, defines privacy as ‘an autonomy or control over the intimacies of personal identity.’⁹ These definitions place the reigns of regulating the conditions of access to an inner private sanctum on an individual.

The second aspect of access and privacy, on which this article will largely focus, is access to information about a person. The term ‘informational privacy’ is relevant to this discourse. For example, authors such as Westin define privacy as the ‘claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.’¹⁰ The notion of an individual’s control over the conditions surrounding access to information about them has collated the debate and frameworks on privacy as predicated on access to information; in this sense, regulation of what

4 BP Knijnenburg and others ‘Introduction and overview’ in BP Knijnenburg and others (eds) *Modern socio-technical perspectives on privacy* (2022) 3.

5 I Altman *The environment and social behaviour: Privacy, personal space, territory, and crowding* (1975); R Gavison ‘Privacy and the limits of law’ (1980) 89 *Yale Law Journal* 423, PJ Wisniewski & X Page ‘Privacy theories and frameworks’ in BP Knijnenburg and others *Modern socio-technical perspectives on privacy* (2022) 21.

6 T Cooley *A treatise on the law of torts, or the wrongs which arise independent of contract* (1888) 29.

7 SD Warren & LD Brandeis ‘The right to privacy’ (1890) 4 *Harvard Law Review* 193.

8 Gavison (n 5) 433.

9 T Gerety ‘Redefining privacy’ (1977) 12 *Harvard Civil Rights-Civil Liberties Law Review* 236. For other definitions of privacy, see H Gross ‘The concept of privacy’ (1967) 42 *NYU Law Review* 34-36.

10 A Westin *Privacy and freedom* (1967) 7. A similar definition is by BN Ellison and others ‘Negotiating privacy concerns and social capital needs in a social media environments’ in S Trepte & L Reinecke (eds) *Privacy online* (2011) 19-21 who define privacy as ‘the ability of individuals to control when, to what extent, and how information about the self is communicated to others.’ Also see J Neethling ‘The concept of privacy in South African law’ (2005) 122 *South African Law Journal* 19.

is retained and what is disclosed from the private to the public realm.¹¹ This definition in itself acknowledges that information about a person may not be in their sole possession or control, but others may have access to one's information. Consequently, a collective responsibility is imposed on others to protect another's right to privacy and unconsented and unreasonable access to their information.¹²

Often, 'privacy' and 'data protection' are used concomitantly and even sometimes synonymously, though discourse on their similarity or identicalness has been contentious.¹³ As definitional purists argue, data protection specifically relates to safeguards emanating from the modalities of processing personal data (information of 'an identified or identifiable natural person'), which may cross the confines of the private sphere that the right to privacy protects.¹⁴ Norms on data protection canvas how information is collected, stored, used and disseminated which has a correlation with the right to privacy but may exceed its formulation in its application.¹⁵ Makulilo concluded that '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.'¹⁶ Notably, some authors have adopted the terms 'data' and 'information privacy' to temper the tension between data protection and privacy conceptualisation.¹⁷ Coalescing concurring and differing debates on privacy and data protection, a common ground that largely unifies the different discourses, is the presence of information and the exercise of control on its disclosure and management. This article underscores the conditions for information disclosure that conform to or conflict with the right to privacy. The ensuing context is characterised by globalisation and revolutionary technological advancements that have opened up frontiers for facilitating access to information and simultaneously complicated the ability of individuals to control information retention and disclosure. The intervention and adaptation of the law to this reality become crucial to protect personal and informational privacy and access to information.

- 11 Wisniewski & Page (n 5) 16-17, X Heng and others *Examining the formation of individual's privacy concerns: Toward an integrative view* (2008).
- 12 H Jia & H Xu 'Measuring individuals' concerns over collective privacy on social networking sites (2016) 10 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 1-2.
- 13 AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) *International Data Privacy Law* 164-165.
- 14 C Cuijpers 'A private law approach to privacy: Mandatory law obliged?' (2007) 4 *Scripted* 312. Art 4 of the General Data Protection Regulation (GDPR) defines personal data as 'any information relating to an identified or identifiable natural person ("data subject")'.
- 15 P de Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxembourg: Constitutionalism in action' in S Gutwirth and others (eds) *Reinventing data protection?* (2009) 3-10.
- 16 Makulilo (n 13) 166.
- 17 PM Schwartz & JR Reidenberg *Data privacy law: A study of United States data protection* (1996) 5; SK Karanja 'Schengen information system and border control co-operation: A transparency and proportionality evaluation' PhD thesis, University of Oslo, 2006 86; LA Bygrave 'Privacy protection in a global context – A comparative overview' (2004) 47 *Scandinavian Studies in Law* 321-322.

3 Reconciling competing interests of privacy and access to information in the United Nations and African legal frameworks

The legal status of the right to privacy evolved from discourse to common law protection to prescriptive with legal recognition and protection in key human rights frameworks such as article 12 of the Universal Declaration of Human Rights (Universal Declaration);¹⁸ article 17 of the International Covenant on Civil and Political Rights (ICCPR); and a majority of national constitutions including on the African continent. Article 17 of ICCPR prohibits 'arbitrary or unlawful interference with' a person's 'privacy, family, home or correspondence', or unlawful attacks on their honour and reputation. The exclusion of privacy rights in the African Charter on Human and Peoples' Rights (African Charter)¹⁹ has inspired discussion on the place of privacy in Africa. Some authors have argued that the omission of the right to privacy in the African Charter should not lead to the conclusion that an individual's right to privacy lacks value in African societies.²⁰ This argument is often grounded in Africa's collectivist culture.²¹ The articulation of the right to privacy in current African legal frameworks challenges arguments on its utility in contemporary African society. Case in point, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which took effect in June 2023, is a homegrown instrument that outlines state obligations with regard to personal data protection.²² Admittedly, the development of the instrument was inspired by European legal frameworks such as the European Union Data Protection Directive 95/46/EC;²³ the Council of Europe Convention 108;²⁴ and the Organisation for Economic Co-operation

18 Universal Declaration of Human Rights, <https://www.ohchr.org/en/human-rights/universal-declaration/translations/english> (accessed 10 August 2024).

19 African Charter on Human and Peoples' Rights, https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf (accessed 5 August 2024).

20 In P Boshe 'A quest for an African concept of privacy', in LA Abdulrauf & H Dube (eds) *Data privacy law in Africa: Emerging perspectives* (2024) 24-26 the author debunks the myth of African privacy as foreign to traditional African societies. Also see AB Makulilo 'Data privacy in Africa: Taking stock of its development after two decades' in LA Abdulrauf & H Dube (eds) *Data privacy law in Africa: Emerging perspectives* (2024) 61 where Makulilo criticises Bygrave and Gutwirth for misinterpreting the absence of a right to privacy provision in the African Charter to mean a devaluation of the individual right to privacy over community interests in S Gutwirth *Privacy and the information age* (2002) 24 and Bygrave (n 17) 328.

21 As above.

22 Malabo Convention, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 5 August 2024). Also see Lawyers Hub 'Africa privacy report 2023/2024: A review of policy trends and digital frontiers in Africa's data protection landscape' (2023), <https://www.ictworks.org/wp-content/uploads/2024/05/Africa-Privacy-Report.pdf> (accessed 5 August 2024).

23 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046> (accessed 5 August 2024).

24 <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (accessed 5 August 2024).

and Development (OECD) Privacy Guidelines.²⁵ All the same, the Malabo Convention addresses privacy and data protection issues in the African context.

Other binding and non-binding instruments have articulated the right to privacy in Africa, such as article 10 of the African Charter on the Rights and Welfare of the Child (African Children's Charter), which protects the right to privacy of children.²⁶ The African Children's Charter, however, was inspired by the UN Convention on the Rights of the Child (CRC), which contains a similar provision.²⁷ Additionally, principle 40 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019 Declaration) articulates everyone's right to privacy and the protection of their personal information.²⁸

Shifting gears to the right to information, its original formulation under international law is under freedom of expression encompassing freedom of expression, right to information, and media freedom. At the UN level, the right to information originates from the freedom of expression definition as the 'freedom to seek, receive and impart information and ideas.'²⁹ Under article 9 of the African Charter, it is simply 'the right to receive information'. Soft law instruments have significantly elaborated the substance of the umbrella of rights encapsulating free expression to peel back the essence of the right to information. General Comment 34 on article 19 of ICCPR, for instance, defines it as the right to access information including records possessed by public bodies or other entities that conduct public functions.³⁰ General Comment 34 proceeds to obligate states to ensure proactive disclosure of information of public interest and the passage of the necessary legal frameworks to enforce the right to information.³¹ Under General Comment 34, one can exercise the right against the state and public bodies. However, successive frameworks have narrowly expanded the scope of duty bearers.

25 For the OECD Privacy Guidelines, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> (accessed 5 August 2024). Also see Makulilo (n 20) 63-64; LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67-97.

26 https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf (accessed 6 August 2024).

27 Preamble to the African Children's Charter and art 16 of CRC, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> (accessed 6 August 2024). Also see A Lloyd 'A theoretical analysis of the reality of children's rights in Africa: An introduction to the African Charter on the Rights and Welfare of the Child' (2002) 2 *African Human Rights Law Journal* 16-17.

28 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/ati/Declaration_of_Principles_on_Freedom_of_Expression_ENG_2019.pdf (accessed 6 August 2024). 'The African Commission on Human and Peoples' Rights first adopted the instrument in 2002. The current 2019 version is a revision of the original Declaration and incorporates stronger protection for freedom of expression and access to information in light of digital advancement.

29 Art 19 ICCPR; art 19 Universal Declaration.

30 General Comment 34 para 18, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf> (accessed 6 August 2024).

31 General Comment 34 para 19.

The right to information under the African Charter is augmented by binding and non-binding instruments that provide context-specific obligations to facilitate access to information. The interdependent character of rights is revealed in the formulation of these provisions with access to information seen as an enabling right to other fundamental rights. For example, article 2 of the African Charter on Democracy, Elections and Governance (African Democracy Charter) links access to information to improved ‘democracy, elections and governance’;³² article 4 of the African Union Convention on Preventing and Combating Corruption includes access to information as a measure towards addressing corruption and related offences;³³ and article 6 of the African Charter on Values and Principles of Public Service and Administration requires the realisation of the right to information in public service and administration towards effective public service delivery.³⁴ An underlying thrust of these instruments is to course-correct and counter the endemic culture of secrecy, maladministration, corruption and impunity in African governments, and enhance transparency, accountability and meaningful public participation.³⁵ The dichotomy between the ensuing secrecy culture in public institutions and contentious secrecy legislation in some African countries against the growing corpus of freedom of information laws in Africa unveils a tension not only within human rights but also within the state and institutional culture.³⁶ Relatedly, Fitzpatrick argues that the ‘tendency of governing elites to confuse “the life of the nation” with “the survival of the regime” creates a grave risk that derogations and limitations on expression and information rights will be excessive.’³⁷

Cognisant of the implication of state secrecy on access to information, the international mechanisms of the UN Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, and the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression adopted

32 Art 2 African Democracy Charter, <https://au.int/sites/default/files/treaties/36384-treaty-african-charter-on-democracy-and-governance.pdf> (accessed 6 August 2024).

33 Art 4 African Union Convention on Preventing and Combating Corruption, https://anticorruption.au.int/sites/default/files/files/2021-06/combatingcorruptionconvention_a5v2enreduced.pdf (accessed 6 August 2024).

34 Art 6 African Charter on Values and Principles of Public Service and Administration, https://au.int/sites/default/files/treaties/36386-treaty-charter_on_the_principles_of_public_service_and_administration.pdf (accessed 6 August 2024).

35 See the Preambles to the instruments in addition to the specific sections.

36 On secrecy laws, see AO Salau ‘The right of access to information and national security in the African regional human rights system’ (2017) 17 *African Human Rights Law Journal* 378; OA Osawe ‘A comparative analysis of the right of access to information under the Nigerian Freedom of Information Act 2011 and the South African Promotion of Access to Information Act 2001’ (2022) 22 *African Human Rights Law Journal* 476-492; J Klaaren ‘The South African “Secrecy Act”: Democracy put to the test’ in H Botha, N Schaks & D Steiger (eds) *The end of the representative state? Democracy at the Crossroads – A German-South African perspective* (2016) 131-156.

37 J Fitzpatrick ‘Introduction’ in S Coliver & P Hoffman (eds) *Secrecy and liberty: National security, freedom of expression and access to information* (1999) xi.

the Joint Declaration on Access to Information and Secrecy Legislation in 2004. The Declaration provides:³⁸

The right of access should be subject to a narrow, carefully tailored system of exceptions to protect overriding public and private interests, including privacy. Exceptions should apply only where there is a risk of substantial harm to the protected interest and where that harm is greater than the overall public interest in having access to the information. The burden should be on the public authority seeking to deny access to show that the information falls within the scope of the system of exceptions.

The right to information under the African Charter is further refined by a tripartite soft law structure found in the 2019 Declaration, the Model Law on Access to Information for Africa (2013 Model Law),³⁹ and the Guidelines on Access to Information and Elections in Africa (2017 Guidelines).⁴⁰ The 2013 Model Law provides that its objective is to give effect to operationalise this right as guaranteed by the African Charter to ‘any information held by a public body or relevant private body; and any information held by a private body that may assist in the exercise or protection of any right’. Crafted in similar terms, the 2019 Declaration and the 2017 Guidelines combined with the 2013 Model Law indeed form the corpus of frameworks that expand the scope of actors upon whom the right of access to information is enforceable.

First, public bodies and relevant private bodies have a duty to proactively disclose information.⁴¹ The proactive disclosure of information principle anticipates that information disclosures are not predicated on a request but are rather done routinely in the course of duty.⁴² Privacy considerations come into play given some of the information held by these bodies may be confidential information or personal data subject to legal protection. Persons can exercise their right of access to information, including access to one’s personal data, against three duty bearers:⁴³

- a public body characterised as an entity established by the Constitution or other law, or is part of government;
- ‘a relevant private body’, meaning an otherwise private body that is owned totally or partially or directly or indirectly ‘controlled or financed by public funds’, or undertakes ‘a statutory or public function or’ service; and

38 Joint Declaration on Access to Information and Secrecy Legislation, <https://www.article19.org/resources/joint-declaration-access-information-secrecy-legislation/> (accessed 6 August 2024).

39 2013 Model Law, https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/model_law_on_ati_in_africa/model_law_on_access_to_information_en.pdf (accessed 6 August 2024).

40 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf (accessed 7 August 2024). The Guidelines were adopted by the African Commission in 2017.

41 Sec 7 2013 Model Law.

42 Part 1 2017 Guidelines.

43 Part 1 sec 1 2013 Model Law.

- a private body but the enforceability of access is conditional upon the exercise or protection of another right.

The presence of a legal framework on privacy and data protection that is concisely drafted, accessible and enforced by competent and independent authorities dovetails with the right to information. There is a reasonable expectation to know to what extent governments can curtail an individual's right to privacy in the name of the right to information as well as the safeguards implemented to prevent arbitrary and unlawful infringement of the right to privacy. General Comment 16 on the right to privacy emphasises the need for information on authorities allowed to interfere with their right to privacy, the manner and extent of the interference and recourse and remedy in the event of a violation.⁴⁴

While the Malabo Convention's objective on personal data commits African states to develop laws to strengthen human rights, especially the protection of physical data and privacy, it attaches a caveat that these measures should not prejudice the free flow of data.⁴⁵ The Malabo Convention and the 2019 Declaration stipulate the guiding principles for the legal processing of personal data, including 'consent and legitimacy, legality and fairness, purpose, adequacy and relevance, accuracy, transparency, and confidentiality and security'.⁴⁶ These principles further demarcate the boundaries of privacy and information access and disclosure. Access to information is also emphasised with regard to the processing of personal information. Among the rights of a data subject in the Malabo Convention and the 2019 Declaration is the right to information on the type, scope, purpose, recipients, and timelines with regard to the information processed about them. The data subject also has the right to access this information and may object to the processing of the data or rectify or erase the information.⁴⁷ Data subjects, therefore, can submit an access to information request to a data controller or processor for their own personal data to manage access to their information.

Also, an examination of the 2019 Declaration shows that from the outset it recognises the correlation between free expression (including the right to information) and privacy towards enabling the right to dignity.⁴⁸ The 2019 Declaration guarantees the right to privacy both offline and online and the protection of personal information under principle 40. The Declaration further outlines state obligations in adopting privacy and data protection laws that comply with international laws and standards.⁴⁹ The balancing and trade-off between privacy, data protection and information disclosure beyond one's private

44 UN Human Rights Committee CCPR General Comment 16: Article 17 (Right to privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation para 6, <https://www.refworld.org/legal/general/hrc/1988/en/27539> (accessed 7 August 2024).

45 Art 8 Malabo Convention.

46 Art 13 Malabo Convention; art 42(2) 2019 Declaration.

47 Art 16 Malabo Convention; Principle 42(3) 2019 Declaration.

48 Preamble to 2019 Declaration.

49 Principle 42 2019 Declaration.

sphere is seen in various provisions. Towards protecting data or information privacy, the Declaration imposes both negative and positive state obligations. The prohibition against ‘indiscriminate and untargeted collection, storage, analysis or sharing of a person’s communications’ and targeted surveillance that contradicts international laws and standards is a negative obligation aimed at ensuring the state respects the right to privacy.⁵⁰ The state’s positive obligation emanates from the duty to adopt laws for ‘the protection of personal information, privacy and communication surveillance of individuals in accordance with international human rights law and standards’ as well as other safeguards.⁵¹

As of August 2024, at least 36 countries in Africa have passed data protection laws.⁵² Fewer countries have adopted access to information laws at about 28 African states.⁵³ Cabo Verde, which was the trendsetter in Africa in adopting data protection laws in 2001, only adopted its access to information law in 2022. Some authors have credited the Brussels Effect as the impetus behind the uptake of domestic data privacy laws in Africa.⁵⁴ Specifically, ‘the adequacy requirement’ under articles 25 to 26 of the now-repealed Data Protection Directive 95/46/EC predicates data transfer to third-party countries on an ‘adequate level’ of protection.⁵⁵ Similarly, the earlier-mentioned influence of the European data protection regime on the substance of the Malabo Convention and many national data protection laws has drawn concern about the absence of an African-centred methodology for regulating privacy and data protection in African countries.⁵⁶ Reflecting that privacy provisions in African constitutions were similarly inspired by the constitutions of imperial governments, it rests on enforcement actors, including the judiciary, to ensure that the interpretation of national statutory provisions is reflective of the African context while protecting fundamental rights such as access to information. This is especially crucial because of concerns over poor implementation of laws despite a demand for public interest information

50 Principle 41 2019 Declaration.

51 Principles 41(2), (3) & 42 2019 Declaration.

52 These are Algeria (2018), Angola (2011), Benin (2009), Botswana (2018), Burkina Faso (2004), Cabo Verde (2001), Chad (2015), Côte d’Ivoire (2013), Egypt (2020), Equatorial Guinea (2016), Eswatini (2022), Gabon (2011), Ghana (2012), Guinea (2016), Kenya (2019), Lesotho (2011), Madagascar (2014), Mali (2013), Mauritania (2017), Mauritius (2017), Morocco (2009), Niger (2017), Nigeria (2023), Republic of Congo (2019), Rwanda (2021), São Tomé & Príncipe (2016), Senegal (2008), Seychelles (2003), Somalia (2023), South Africa (2013), Tanzania (2022), Togo (2019), Tunisia (2004), Uganda (2019), Zambia (2021), Zimbabwe (2021). Ethiopia, Malawi and Namibia have draft laws. ALT Advisory ‘Which African countries have a data protection law?’, <https://dataprotection.africa/which-african-countries-have-a-data-protection-law/> (accessed 8 August 2024).

53 These are Angola, Benin, Burkina Faso, Cabo Verde, Côte d’Ivoire, Ethiopia, Ghana, Guinea, Kenya, Liberia, Malawi, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Seychelles, Sierra Leone, South Africa, South Sudan, Sudan, Tanzania, Togo, The Gambia, Tunisia, Uganda, Zambia and Zimbabwe. AFIC ‘Access to information laws in Africa’, <https://www.africafoicentre.org/foi-laws/?cp=3> (accessed 8 August 2024).

54 Boshe (n 20) 23; Makulilo (n 20) 69-71; Makulilo (n 13) 42-50.

55 As above.

56 G Greenleaf & B Cortier ‘Comparing African data privacy laws: International, African and regional commitments’ University of New South Wales Law Research Series (2020) 33; Boshe (n 20) 30-34.

and privacy and data protection in Africa.⁵⁷ In subsequent parts, this article analyses how courts in Kenya and South Africa have confronted this conundrum.

3.1 The contribution of the African Commission 2017 Guidelines to the information versus privacy debate and its implementation in South Africa and Kenya

The Guidelines on Access to Information and Elections were adopted by the African Commission on Human and Peoples' Rights (African Commission) in 2017 to reinforce the protection of the right to freedom of expression and access to information particularly during elections.⁵⁸ The 2017 Guidelines underscore 'the principle of proactive disclosure of information' throughout the election period as a conduit for enhanced accountability of electoral stakeholders and promoting credibility, integrity and stability during African elections.⁵⁹ The interdependence between access to timely, credible, relevant and accurate information with meaningful political participation is an underlying thrust of the 2017 Guidelines. Meaningful political participation, including exercising the right to vote, envisages the active participation of an informed electorate in the elections and other democratic processes who can freely exercise their right to expression, association and assembly.⁶⁰

The realisation of access to information during elections transforms voting from a passive exercise to an engaging experience by informed voters. That being said, various historical, social, cultural, political and economic considerations and biases influence voter choice in many African elections that are not anchored on issues. Blind affiliation to group interests driven by ethnicity, tribe and religion, among others, or personality politics without a corresponding reflection on issues and track record are an Achilles heel of meaningful participation in elections in Africa.⁶¹ Arguably, through concerted civic and voter education and access to

57 A Okello, S Sunderland & J Asunka 'Veiled transparency: Access to public information remains elusive despite progress on right-to-information laws' (22 February 2024) 771 *Afrobarometer* 3, <https://www.afrobarometer.org/wp-content/uploads/2024/02/AD771-PAP10-Access-to-public-information-remains-elusive-across-Africa-Afrobarometer-20feb24.pdf> (accessed 9 August 2024); CIPESA 'Mapping and analysis of privacy laws in Africa' (2021), https://cipesa.org/wp-content/files/briefs/Mapping_and_Analysis_of_Privacy_Laws_in_Africa_2021.pdf (accessed 9 August 2024).

58 Rationale and objectives of the Guidelines.

59 As above.

60 UN Human Rights Committee General Comment No 25: The right to participate in public affairs, voting rights and the right of equal access to public service (art 25) paras 8, 9 & 12, <https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf> (accessed 9 August 2024). Also see *President of the Republic of South Africa & Others v M & G Media Ltd* CCT 03/11 [2011] ZACC 32; 2012 (2) BCLR 181 (CC); 2012 (2) SA 50 (CC) (29 November 2011), <https://www.saflii.org/za/cases/ZACC/2011/32.html> (accessed 9 August 2024); *My Vote Counts NPC v Minister of Justice and Correctional Services & Another* CCT249/17 [2018] ZACC 17; 2018 (8) BCLR 893 (CC); 2018 (5) SA 380 (CC) (21 June 2018) (*MVC 2018*) para 34, https://www.saflii.org/za/cases/ZACC/2018/17.html#_ftn29 (accessed 9 August 2024).

61 JT Andrews & K Inman 'Explaining vote choice in Africa's emerging democracies' (2009) Conference Paper - 2009 meeting of the Midwest Political Science Association, <https://fsi->

information, fledgling African democracies can course-correct and nurture a culture of issue and performance-based voter choice.

Uniquely, the 2017 Guidelines identify eight key electoral stakeholders and outline the information which, at the minimum, they should disclose to the electorate and public during elections. The electoral stakeholders are ‘appointing authorities of election management bodies (EMBs), EMBs, political parties and candidates, civil society organisations (CSOs), law enforcement agencies, media regulatory bodies, media and online media platform providers, and election observers and monitors.’

Since 2019, the Centre for Human Rights, University of Pretoria (CHR) has undertaken a country assessment of domestic compliance with the Guidelines that covered South Africa (2019),⁶² Uganda (2020),⁶³ The Gambia (2021)⁶⁴ and Kenya (2022).⁶⁵ While there are varying levels of compliance in the different countries influenced by democratic culture, legislative coherence, institutional strength, and resource capacity, among others, the reports reveal an overall need to enhance knowledge of the Guidelines and promote its mainstreaming in the activities of electoral stakeholders.⁶⁶ Guidelines 31 to 34 strive to promote the implementation of the 2017 Guidelines by mandating state adoption of ‘legislative, administrative, judicial and other measures’ to implement the soft law. States are also required to disseminate the Guidelines to relevant electoral stakeholders and ensure effective training. Compliance measures should be captured in the periodic country reports ‘submitted to the African Commission under article 62 of the African Charter’.

Relevant to privacy, data protection and access to information, the CHR reports, as well as advocacy actions on the implementation of the proffered recommendations, reveal instances of conflict between access to information and privacy and data protection obligations. A review of the Guidelines reveals a singular focus on information disclosure. The Guidelines are structured to outline the categories of information electoral stakeholders should disclose

live.s3.us-west-1.amazonaws.com/s3fs-public/evnts/media/Andrews_Inman_Explaining_Vote_Choice_in_African_Democracies.pdf (accessed 11 August 2024).

62 CHR and others ‘Proactive disclosure of information and elections in South Africa’ (2020), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Proactive_Disclosure_of_Information_and_Elections_in_South_Africa.pdf (accessed 11 August 2024).

63 PD Mutesasira & DR Ruhweza ‘Proactive disclosure of information and elections in Uganda’ (2023), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Proactive_Disclosure_of_Information_During_Elections_Uganda.pdf (accessed 11 August 2024).

64 J Grey-Johnson ‘Proactive disclosure of information and elections in The Gambia’ (2023), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Proactive_Disclosure_of_Information_During_Elections_Gambia.pdf (accessed 11 August 2024).

65 L Mute ‘Proactive disclosure of information and elections in Kenya’ (2023), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Proactive_Disclosure_of_Information_During_Elections_Kenya.pdf (accessed 11 August 2024).

66 Insights from electoral stakeholder engagements organised by the CHR in which the author of this article facilitated as a project lead.

during the elections. Not surprisingly, EMBs bear the most burden in information disclosure on both internal records as well as other election records, given their election administration mandate.⁶⁷ The potential dilemma of conflicting proactive disclosure obligations with privacy and data protection does not receive a mention in the Guidelines. This is not to say that the Guidelines did not contemplate the notion of competing rights. For example, the stipulation for responsible authorities to refrain from implementing internet shutdowns further provides that in exceptional cases necessitating an internet shutdown, the reasons shall be proactively disclosed and the limitation complies with the three requirements of lawfulness, legitimate aim and necessity and proportionality in addition to prior judicial review.⁶⁸ Interestingly, among the stakeholders, the Guidelines only indicate a general caveat on proactive disclosure duties of CSOs and this is based on exceptional cases where it is evident that their operations may suffer demonstrable harm.⁶⁹

Political parties are also data controllers and data processors during elections. The 2017 Guidelines perceive political parties through the lens of a duty bearer to disclose information with no mention of their privacy and data protection obligations. Guideline 21 requires states to enact the relevant laws including on the proactive disclosure by political parties of received public and private funding, campaign expenditures, and annual audited financial reports. The orientation of political parties has traditionally been categorised under private bodies but their status as private bodies blurs when some elements of a public body breach this boundary such as through the receipt of public funds.⁷⁰ In South Africa, courts have affirmed the position of political parties as voluntary associations and private bodies.⁷¹ However, in their capacity as private bodies, they have information disclosure obligations including on private funding, that the Constitutional Court of South Africa linked to the electorate's ability to meaningfully exercise their right to vote and make informed decisions.⁷² This obligation also extends to independent candidates. In the fulfilment of this obligation, political parties and candidates may disclose personal data about private funders which, in some cases, may lead to prejudices emanating from supporting certain parties or candidates. In South Africa, the decision of the Constitutional Court led to the amendment of the Promotion of Access to Information Act (PAIA),⁷³ and the adoption of the

67 Guidelines 13-19 2017 Guidelines.

68 Guidelines 26-28 2017 Guidelines.

69 Guideline 30 2017 Guidelines.

70 I Biezen 'Political parties as public utilities' (2004) 10 *SAGE* 7021-702; A Gauja 'Political parties: Private associations or public utilities?' in J Gardner (ed) *Comparative election law* (2022) 177-192.

71 *Institute for Democracy in South Africa & Others v African National Congress & Others* (9828/03) [2005] ZAWCHC 30; 2005 (5) SA 39 (C); [2005] 3 All SA 45 (C); 2005 (10) BCLR 995 (C) (20 April 2005) (*IDASA v ANC*), <https://www.saflii.org/za/cases/ZAWCHC/2005/30.html> (accessed 11 August 2024).

72 MVC 2018 (n 60) paras 33 & 48. The MVC decision overturned the decision in *IDASA v ANC* (n 71) that exempted political parties from disclosing private funding by nature of their private body status.

73 PAIA Amendment Act 31 of 2019, https://www.gov.za/sites/default/files/gcis_document/202007/43388gon630.pdf (accessed 11 August 2024).

Political Party Funding Act (PPFA) in 2018 which fulfils Guideline 21. In Kenya, section 16 of the Election Campaign Financing Act, 2013⁷⁴ regulates disclosure of funding by political parties. However, the Act's implementation has suffered in the wake of its suspension from coming into force until the 2017 elections and lack of political will.⁷⁵

Instances in the Guidelines that necessitate privacy considerations include on disclosure of the voter register. Guideline 17 obligates EMBs to proactively disclose the voter's register with voter's identification information including their full name, identity card number, picture (if available), age and gender. Data protection considerations require EMBs and other data controllers and processors to consider data protection principles, particularly purpose limitation and data minimisation before disclosing such personal details in the full register. Therefore, it is important to read these provisions together with international privacy and data protection standards, and relevant national laws and case law.

National legislation is important to balance privacy and access to information during elections. In Kenya, the Independent Electoral and Boundaries Commission (IEBC) is obligated to apply the data protection principles as outlined in the Data Protection Act in processing the personal data of voters.⁷⁶ The voter's roll contains biometric data as well as other personal information including their name, identity number, sex, postal and residential address, and phone and email contact details.⁷⁷ South Africa's voter's register contains the identity number, consecutive number, voter's name and voter's address or ordinary residence but no mention of a photograph.⁷⁸ A participating political party can request a copy of the voter's roll without charge but will be subject to a fee if they want the version with additional information on the addresses of voters.⁷⁹ They are also tasked to only use the information for election purposes, failing which they are guilty of an offence.⁸⁰ This makes political parties data controllers and processors with responsibilities to protect the privacy and data of voters.

74 42 of 2013, <https://www.iebc.or.ke/uploads/resources/SrIIWeBWMH.pdf> (accessed 11 August 2024).

75 G Ndirangu 'No limits: Campaign spending spikes ahead of Kenyan elections' *Al Jazeera* 22 June 2022, <https://www.aljazeera.com/features/2022/6/22/no-limits-campaign-spending-spikes-ahead-of-kenyan-elections> (accessed 12 August 2024); Mzalendo 'Campaign financing legislation and the 2022 general elections', <https://mzalendo.com/posts/campaign-financing-legislation-and-the-2022-general/> (accessed 12 August 2024). See also Election Campaign Financing (Amendment) Bill, 2020, <https://www.iebc.or.ke/uploads/resources/iGNrE6ZL95.pdf> (accessed 12 August 2024).

76 Sec 25(i) IEBC Act 9 of 2011, <https://www.iebc.or.ke/uploads/resources/8Z5fmROhVD.pdf> (accessed 8 August 2024).

77 Sec 8 The Elections (Registration of Voters) Regulations, <http://kenyalaw.org:8181/exist/kenyalex/sublegview.xml?subleg=CAP.%207#doc-0> (accessed 8 August 2024).

78 Regulation 10 Voter Registration Regulations 1998 as amended, https://www.gov.za/sites/default/files/gcis_document/202402/50066gon4307.pdf (accessed 12 August 2024).

79 Regulation 8 Voter Registration Regulations, 1998 as amended.

80 Sec 16(4) Electoral Act as amended, <https://www.gov.za/documents/electoral-act> (accessed 12 August 2024).

Privacy and data protection responsibilities of political parties are heightened in the information age. Digital technologies have refined data-driven political campaigning and strategising that has raised concerns around the data of voters and the wider public.⁸¹ A breach into the private sphere is evident in the growing trend of unsolicited and targeted political messaging during elections sent through personal devices or social media platforms.⁸² Increasing integration of technology in election administration in Africa coupled with empirical evidence of data breaches of voter information, as in the case of Kenya in the 2022 elections,⁸³ or closed political party lists information, as was the case in South Africa during the 2024 elections⁸⁴ reveal a need for electoral stakeholders to reinforce data privacy practices in compliance with existing legislation. Information Regulators and Data Protection Authorities have adopted regulations to address the tensions of access to information and privacy. The Office of the Data Protection Commissioner (ODPC) in Kenya published the Guidance Note on the Processing of Personal Data for Electoral Purposes during the 2022 election period, aimed at guiding data processors, including political parties and candidates.⁸⁵ In 2019, the South Africa Information Regulator published a Guidance Note on the Processing of Personal Information of a Voter by a Political Party in Terms of the Protection of Personal Information Act, 4 of 2013.⁸⁶ However, there is a need for better compliance and wider civic education on information and privacy rights.⁸⁷

81 CJ Bennett & D Lyon 'Data-driven elections' (2019) 8 *Internet Policy Review* 3-4.

82 Privacy International 'Challenging data exploitation in political campaigning' (2020) 5-6, https://privacyinternational.org/sites/default/files/2020-06/PI%20Recs_Challenging%20Data%20Exploitation%20in%20Political%20Campaigning.pdf (accessed 12 August 2024).

83 J Otieno 'Kenyans protest registration as party members without consent' *The Star* 19 June 2021, <https://www.the-star.co.ke/news/2021-06-19-kenyans-protest-registration-as-party-members-without-consent/> (accessed 12 August 2024). Also see R Mosero 'In Kenya's 2022 elections, technology and data protection must go hand in hand' Carnegie Endowment for International Peace (8 August 2022), <https://carnegieendowment.org/2022/08/08/in-kenyas-2022-elections-technology-and-data-protection-must-go-hand-in-hand-pub-87647> (accessed 12 August 2024).

84 A Moyo 'IEC fires official for leaking political candidate lists' *IT Web* 12 March 2024, <https://www.itweb.co.za/article/iec-fires-official-for-leaking-political-candidate-lists/xnkIQz1AKjM4Ymz> (accessed 12 August 2024).

85 Mosero (n 83). The original Guidance Note was no longer available on the ODPC's website at the time of writing this article.

86 <https://info regulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-PolParties-1.pdf> (accessed 13 August 2024).

87 IR 'Information Regulator shares outcomes of complaints investigated and assessments conducted in relation to PAIA and POPIA' (26 March 2024), <https://info regulator.org.za/wp-content/uploads/2020/07/MEDIA-BRIEFING-STATEMENT-OF-THE-INFORMATION-REGULATOR-ON-OUTCOMES-ON-COMPLAINTS-ASSESSMENTS.pdf> (accessed 13 August 2024). Also see MA Bouke and others 'African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions' (2023) *arXiv* 6, <https://arxiv.org/pdf/2307.01966> (accessed 13 August 2024).

4 The interplay of privacy, data protection and access to information in the broader legal framework in South Africa and Kenya

Both South Africa and Kenya have adopted access to information and data protection laws and set up the required enforcement agencies. Arguably, South Africa is more advanced in anchoring these laws through supporting policies, institutions and case law though the effectiveness of implementation has been contentious.⁸⁸ South Africa heralded the adoption of information laws in Africa with the enactment of PAIA in 2000.⁸⁹ The Act was operationalised in 2001. PAIA is the statute envisioned under article 32(2) of the Constitution to enable access to information in the possession of the 'state, or another person' and that is necessary for 'the exercise or protection of any rights'.⁹⁰ The status of the legislation in relation to article 32 has been interpreted in the courts of law with PAIA affirmed as the vehicle for facilitating the constitutional right of access to information.⁹¹ Further access to information is endorsed as a means towards reinforced 'human rights culture, social justice, transparency, accountability and effective governance of all public and private bodies'.⁹² From the outset, the absolute character of access to information is negated with PAIA subjecting the exercise of the right to justifiable limitations including 'the reasonable protection of privacy, commercial confidentiality, and effective, efficient and good governance' and such as to balance access to information with any other rights.⁹³ Relevant to the crux of this article, the below focuses on the extent privacy rights may warrant the restriction of access to information.

Assessing the bounds of information disclosure within the confines of the law requires enforcement agencies to consider access to information frameworks alongside privacy and data protection laws; relevant to South Africa, PAIA and the Protection of Personal Information Act (POPIA). This is crucial to safeguard against unreasonable information disclosure as articulated under section 34 of PAIA.⁹⁴ In an effort to reconcile the interests of access to information and privacy rights, PAIA outlines either mandatory or discretionary obligations in disclosing

88 DL Marais, M Quayle & JK Burns 'The role of access to information and public participation in governance: A case study of access to policy consultation records in South Africa' (2017) 9 *African Journal of Public Affairs* 36-49; MG Mojapelo 'A framework towards the implementation of freedom of information legislation in South Africa' (2024) *Emerald Insight*, <https://www.emerald.com/insight/content/doi/10.1108/IDD-11-2022-0121/full/pdf?title=a-framework-towards-the-implementation-of-freedom-of-information-legislation-in-south-africa> (accessed 13 August 2024).

89 PAIA https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf (accessed 13 August 2024).

90 Art 9(A) PAIA.

91 *IDASA v ANC* (n 71); *Kerkhoff v Minister of Justice and Constitutional Development & Others* 2011 (2) SACR 109 (GNP) [2010] ZAGPPHC 5; 14920/2009 (10 February 2010), <https://www.saflii.org/za/cases/ZAGPPHC/2010/5.html> (accessed 13 August 2024).

92 Secs 9(c) & (e) PAIA.

93 Sec 9(b) PAIA.

94 Also see the judgment in *Smuts NO & Others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & Others*

certain information that is protected from disclosure on privacy grounds. For both public and private bodies, considerations include ‘unreasonable disclosure of third party information of a natural person including a deceased person’;⁹⁵ third party commercial information such as trade secrets or own commercial information in the case of a private body;⁹⁶ breach of confidentiality or disclosure that may threaten the receipt of future confidential information for a public body;⁹⁷ protection of the safety of persons or property;⁹⁸ unwaived legal privilege considerations;⁹⁹ and protection of research data of a third party, or research data of the public or private body.¹⁰⁰

Other privacy considerations and exemptions from disclosure for a public body on privacy grounds include some records of the South African Revenue Service (SARS) unless requested by the tax subject or their representative;¹⁰¹ police records ‘in bail proceedings, and law enforcement and legal proceedings’;¹⁰² reasonable threats to the national defence, security and international relations;¹⁰³ material threats to national economic interests and financial welfare and the public body’s commercial activities;¹⁰⁴ impediments to the formulation or success a policy, or public decision making;¹⁰⁵ and ‘manifestly frivolous or vexatious requests’ or requests that may considerably and unreasonably redirect resources.¹⁰⁶

While PAIA stipulates specific exemptions to these considerations, it also provides a general public interest override with regard to grounds of refusal based on privacy except concerning SARS records under section 35 of PAIA.¹⁰⁷ In particular, the public interest override operates if information disclosure reveals a substantial legal offence or violation; or ‘imminent and serious public safety or environmental risk’.¹⁰⁸ Further, the enforcement agency must weigh whether the public interest in the information disclosure supersedes the contemplated harm.

Kenya’s Access to Information Act (ATI), on the other hand, is a fairly recent enactment having come into force in 2016.¹⁰⁹ The equally important

(1199/2021) [2022] ZAECKMHC 42 (26 July 2022) paras 41–43, <https://www.saflii.org/za/cases/ZAECKMHC/2022/42.html> (accessed 13 August 2024).

95 Secs 34 & 63 PAIA.

96 Secs 36, 64 & 68 PAIA.

97 Secs 37 & 65 PAIA.

98 Secs 38 & 66 PAIA.

99 Secs 40 & 67 PAIA.

100 Secs 43 & 69 PAIA.

101 Sec 35 PAIA.

102 Sec 39 PAIA.

103 Sec 41 PAIA.

104 Sec 42 PAIA.

105 Sec 44 PAIA.

106 Sec 45 PAIA.

107 Secs 46 & 70 PAIA

108 As above.

109 ATI Act, <http://kenyalaw.org/8181/exist/kenyalex/actview.xql?actid=CAP.%207M> (accessed 14 August 2024).

Data Protection Act (DPA) became law in 2019.¹¹⁰ The ATI Act similarly operationalises the right of access to information under article 35 of Kenya's Constitution. The formulation of article 35(1) is identical to that of South Africa's article 32(1). However, article 35 goes further to guarantee the right to 'the correction or deletion of untrue or misleading information that affects the person' and obligates the state to 'publish and publicise any important information affecting the nation.'¹¹¹

Comparatively, the ATI Act's attempt to reconcile the competing interests on access to information and privacy, while not as elaborate as PAIA, is couched in similar themes. In rather broad terms, access to information shall be limited to protect national security; 'due process of law; the safety, health or life of a person'; unjustified privacy violation of another; substantial prejudice to the commercial interests of 'the data subject or a third party'; damage to a 'public entity's position in any actual or contemplated legal proceedings'; or professional confidentiality.¹¹² The ATI Act also provides a general public interest override requiring information disclosure by 'a public or private body where the public interest in information disclosure outweighs the harm to protected interests' subject to a court's determination.¹¹³ Additionally, considerations of individual privacy and commercial interests do not apply 'if a request for information relates to the results of any product or environmental testing, and the information concerned reveals a serious public safety or environmental risk'.¹¹⁴

4.1 Judicial interpretation of the balance between access to information and privacy rights in South African and Kenyan courts

The legal systems in Kenya and South Africa are mixed, including both statute and common law pronouncements.¹¹⁵ Common law is defined as law emanating from judicial decisions as opposed to statutes. In *Marbury v Madison* the United States Supreme Court stated: 'It is emphatically the province and duty of the judicial department to say what the law is. Those who apply the rule to particular cases, must of necessity expound and interpret that rule.'¹¹⁶ Courts have a legal interpretive mandate that has been defined as 'the process or activity of using legal materials, such as statutes, constitutions, contracts, wills, and the like, to ascertain

110 DPA, <http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20411C> (accessed 14 August 2024).

111 Arts 35(2) & (3) Constitution of Kenya, <https://kenyalaw.org/kl/fileadmin/pdfdownloads/TheConstitutionOfKenya.pdf> (accessed 14 August 2024).

112 Secs 6(1)(d), (e), (h & i) ATI Act.

113 Sec 6(4) ATI Act.

114 Sec 6(3) ATI Act.

115 WPR 'Common law countries 2024', <https://worldpopulationreview.com/country-rankings/common-law-countries> (accessed 14 August 2024).

116 *Marbury v Madison* 5 US 137, 177, 2 L Ed 60 (1803), <https://supreme.justia.com/cases/federal/us/5/137/> (accessed 14 August 2024).

legal obligations, powers, rights, privileges, and so on'.¹¹⁷ In other definitions, interpretation 'refers to the activity of the judge who, on the one hand, attempts to determine the scope of an ambiguous or obscure text and, on the other hand, attempts to elaborate a solution when the text presents a gap'.¹¹⁸ South African and Kenyan courts have faced the task of dispelling the tensions in the statutory articulations of access to information and privacy rights in social contexts towards both determining the scope of the law, filling gaps and/or aligning the law to the spirit of the Constitution.

In *Arena Holdings* South Africa's Constitutional Court was confronted with a challenge to the constitutionality of the absolute exemption of taxpayer records from disclosure under section 35 of PAIA.¹¹⁹ The case emanated from a refusal by SARS to accede to a 2019 request for the tax records of the former President, Jacob Zuma, following allegations that he evaded taxes during his tenure as President.¹²⁰ SARS denied the request because the records were confidential and exempted from disclosure as per sections 34(1) and 35(1) of PAIA, and section 69(1) of the Tax Administration Act (TAA).¹²¹ The Court had a duty to balance the competing interests between the personal 'right to privacy of taxpayer records' against the public interest in accessing the records where there is evidence of serious illegality.¹²²

The Constitutional Court had previously applied public interest considerations in ruling against the absolute prohibition of information disclosure on privacy grounds involving divorce proceedings¹²³ and asylum applications.¹²⁴ In confirming the order of the High Court on the unconstitutionality of the absolute prohibition under section 35 read together with section 46 of PAIA in *Arena Holdings*, the Constitutional Court asserted that the absolute exemption of individual tax records was not a less restrictive measure to limiting the right of disclosure.¹²⁵ The absolute approach contradicted the constitutional approach to competing rights. The Court added that applying the public interest override provided under section 46 of PAIA to the mandatory protection of taxpayer

117 M Greenberg 'Principles of legal interpretation' (2016), <https://philosophy.ucla.edu/wp-content/uploads/2016/08/Principles-of-Legal-Interpretation-2016.pdf> (accessed 14 August 2024).

118 A Rieg 'Judicial interpretation of written rules' (1979) 40 *Louisiana Law Review* 49. Also see F Geny *Method of interpretation and sources of private positive law* (1963).

119 *Arena Holdings (Pty) Limited v/a Financial Mail & Others v South African Revenue Service & Others* CCT365/21 (*Arena Holdings v SARS*) para 6, <https://collections.concourt.org.za/bitstream/id/62514/%20Judgment%20CCT%20365-21%20Arena%20Holdings%20and%20Others%20v%20SARS%20and%20Others.pdf> (accessed 14 August 2024).

120 As above.

121 *Arena Holdings* (n 119) para 7.

122 *Arena Holdings* (n 119) para 134.

123 *Johncom Media Investments Limited v M & Others* (CCT 08/08) [2009] ZACC 5; 2009 (4) SA 7 (CC); 2009 (8) BCLR 751 (CC) (17 March 2009), <https://www.saflii.org/za/cases/ZACC/2009/5.pdf> (accessed 14 August 2024).

124 *Mail and Guardian Media Ltd & Others v Chipu NO & Others* (CCT 136/12) [2013] ZACC 32; 2013 (11) BCLR 1259 (CC); 2013 (6) SA 367 (CC) (27 September 2013) paras 164 & 166, <https://www.saflii.org/za/cases/ZACC/2013/32.html> (accessed 14 August 2024).

125 *Arena Holdings* (n 119) para 171.

information would still ensure the protection of confidentiality as the disclosure would be limited and closely defined; the principle of severability would operate to demarcate the limits of disclosure; and the taxpayer would retain a right of notice, response and appeal.¹²⁶

The order by the Constitutional Court in *Arena Holdings* not only obligated Parliament to address the constitutional conflict in the contentious provisions but went a step further in providing, in the interim, an amended wording to the contentious provisions that applies the public interest override to section 35 of PAIA's confidentiality provisions.¹²⁷

Kenyan courts similarly have confronted questions on the privacy of taxpayers' records when faced with access to information demands in *Njoya*.¹²⁸ In the Court of Appeal case, the Kenya Revenue Authority (KRA) denied a request for information on whether members of parliament were paying taxes on the ground that it violated confidentiality under section 125 of the Income Tax Act.¹²⁹ The applicant challenged the constitutionality of the provisions with regard to article 35(1)(b) of the Constitution. In allowing the appeal, the Court of Appeal stated:¹³⁰

It is true to say that traditionally confidentiality of tax information is a globally recognised and accepted concept which is meant to be an aid in compliance ... Still, we entertain no doubt that the right to information is critical to the attainment of transparent and accountable government and is an enabler to the exercise and enjoyment of other rights by citizens. It has been recognised expressly in the Constitution of Kenya 2010, under article 35.

Notably, since the decision was made, the Income Tax Act was repealed by the Tax Procedures Act, effective as of January 2016.¹³¹ Both events preceded the adoption of the ATI Act in Kenya. Two facts stand out: Unlike PAIA, the ATI Act does not expressly exempt the confidentiality of tax records from access to information requests under section 6. However, the Tax Procedures Act in stipulating exemptions to the confidentiality of taxpayer records excludes an information request that meets the public interest override standard.¹³² It would be advisable for the Kenyan courts to learn from its South African counterparts in the provision of orders and provide further guidance to Parliament to cure the legislative anomaly where relevant. For example, South Africa's Constitutional

126 *Arena Holdings* (n 119) para 193.

127 *Arena Holdings* (n 119) paras 205(2) and (3).

128 *Timothy Njoya v Attorney General* Civil Appeal 112 of 2015 [2017] eKLR (*Njoya*), <https://kenyalaw.org/caselaw/cases/view/141660/> (accessed 14 August 2024).

129 *Njoya* (n 128) 1. The Income Tax Act was replaced by the Tax Procedures Act 29 of 2015, <http://kenyalaw.org:8181/exist/kenyalex/actview.xml?actid=CAP.%20469B> (accessed 14 August 2024). The confidentiality provisions and allowable exemptions are provided under sec 6.

130 *Njoya* (n 128) 5.

131 Act 29 of 2015, <http://kenyalaw.org:8181/exist/kenyalex/actview.xml?actid=CAP.%20469B> (accessed 15 August 2024).

132 Sec 6 TPA.

Court amended the wording of the impugned provision pending parliamentary action. This allowed, on the one hand, guidance on a constitutionally aligned wording of the section and, on the other, protection of the doctrine of separation of powers.¹³³

After the passage of the ATI Act, Kenyan courts have affirmed the importance of maximum disclosure in the interest of the public in light of section 6 exemptions that consider the right to privacy. In *Zebedeo John Oporo v The Independent Electoral and Boundaries Commission*¹³⁴ the respondent denied an information request on certain information about a parliamentary seat election including the number of voters identified electronically, copies of polling station voter identification and verification forms, and polling station diaries. The IEBC rejected the request on grounds of privacy. However, in allowing the petition the High Court stated:¹³⁵

The fact that the information falls within the list of legitimate exception grounds is not sufficient to exempt it from disclosure. The disclosure must harm the specific interest substantially and this harm must be greater than the public interest in receiving the information. Disclosure takes precedence over secrecy, and to give effect to the principle of maximum disclosure, any legislation or provision contradicting this principle should be construed narrowly and in favour of the enforcement of the right.

In yet another case, *Tiso Blackstar Group (Pty) Ltd & Others v Steinhoff International Holdings NV*, the issue of legal privilege as a barrier to access to information was litigated at the Western Cape High Court.¹³⁶ The case arose from a refusal to honour an access to information request for an investigative report on accounting irregularities by the respondent, Steinhoff International Holdings NV, a public company. The applicants in this case are a media house and a civil society organisation. The public interest motivation behind the request was to accurately report on a public interest matter which, in this case, was the corporate scandal.¹³⁷ Access was denied on the grounds of legal privilege under section 67 of PAIA.¹³⁸ According to Steinhoff, the report that was the subject of the information request was prepared expressly to seek legal advice for actual or contemplated litigation. For a record to meet the test of litigation privilege, the document in question ‘must have been obtained or brought into existence for the purpose of a litigant’s submission to a legal advisor for legal advice; and second that litigation was pending or contemplated as likely at the time’.¹³⁹ In this

133 *Arena Holdings* (n 119) paras 205(2) and (3).

134 *Zebedeo John Oporo v The Independent Electoral and Boundaries Commission* [2017] eKLR (Oporo) para 39, <http://kenyalaw.org/caselaw/cases/view/140609> (accessed 15 August 2024).

135 *Oporo* (n 134) para 39.

136 *Tiso Blackstar Group (Pty) Ltd & Others v Steinhoff International Holdings NV* (18706/2019) [2022] ZAWCHC 265; 2023 (1) SA 283 (WCC) (10 May 2022) (*Blackstar*), <https://www.saflii.org/za/cases/ZAWCHC/2022/265.html> (accessed 15 August 2024).

137 *Blackstar* (n 136) para 10.

138 *Blackstar* (n 136) para 11.

139 *Competition Commission of South Africa v Arcerlormittal South Africa Ltd & Others* (680/12) [2013] ZASCA 84; [2013] 3 All SA 234 (SCA); 2013 (5) SA 538 (SCA); [2013] 1 CPLR

case, the respondent's claim of litigation privilege failed to meet the prescribed standard and the Court nullified the refusal.¹⁴⁰

From the above selected cases, a trend emerges from Kenyan and South African courts to narrowly construe privacy restrictions when faced with a conflict with access to information in the interest of the public. This is especially so when the information is in the control of a public body, or a private body and necessary for the exercise of a right. Laudably, this is important towards promoting good governance, transparency and accountability in public and private institutions.

5 Conclusion

The quest towards finding the equilibrium between privacy and access to information is complex and multifaceted requiring the intervention of legal frameworks at international, regional and domestic levels, and various enforcement actors including the judiciary. However, crucial instruments on the African continent, such as the African Commission's 2017 Guidelines on Access to Information and Elections in Africa, while impressively advancing access to information, have gaps with regard to the corresponding privacy and data protection rights. This article's analysis of the soft law instrument shows the importance of a holistic reading of international, regional and national law protections to balance access to information and privacy rights. South Africa and Kenya have made strides in confronting this rights conflict in their legal systems. Where a conflict emerges concerning balancing access to information and privacy, the laws and courts have underscored public interest disclosure considerations that supersede the potential harm of disclosure. Arguably, this approach, which eschews rights absolutism, allows for the better entrenchment of disclosure practices, good governance, accountability and transparency that has historically marred national democratic trajectories in African countries.

1 (SCA) (31 May 2013) para 21, <https://www.saflii.org/za/cases/ZASCA/2013/84.html> (accessed 15 August 2024).

140 *Blackstar* (n 136) para 70.