1-1-2022

Law and recordkeeping: A tale of four African countries

Darra Hofman
San Jose State University, darra.hofman@sjsu.edu

Shadrack Katuu
University of South Africa

Recommended Citation

Darra Hofman and Shadrack Katuu. "Law and recordkeeping: A tale of four African countries" *Managing Digital Records in Africa* (2022): 7-48. https://doi.org/10.4324/9781003203155-2

1 Law and recordkeeping

A tale of four African countries

Darra Hofman and Shadrack Katuu

Introduction

Archives and records management (ARM) professionals are inescapably entangled with the law. After all, the law may dictate what records must be created, their form, who may access them, their retention, and their eventual disposition. In each archival function, from selection and appraisal to referencing and access, the ARM professional must consider not only archival principles, but also legal requirements, putting an archivist without legal training in the position, for example, of determining what records fall within the scope of an access to information (ATI) request. This challenge is made more complex by the fact that the law rarely contemplates records as records, but rather as documents, information, and evidence. This chapter is based on an examination of major legal and regulatory instruments[1] related to records and archives management in Botswana, Kenya, South Africa, and Zimbabwe, undertaken to provide grounded, evidence-informed guidance for both practitioners and educators tasked with the responsibility of implementing recordkeeping. It should be noted, however, that a complete analysis of all the potential laws and regulations for each country was beyond the scope of this chapter. Furthermore, in those countries with elements of common law (discussed in greater detail *infra*), which include all of the countries in this study, judicial decisions ("case law") are of central importance in interpreting and implementing codified law; a full analysis of case law was also beyond the scope of this work. Nonetheless, this study identified major trends at the intersection of law and records, as well as archives, in the countries under study and may serve as a useful point of departure for ARM professionals in those countries and beyond for benchmarking.

Law as a system

"Those who have tried to define *law* agree only that no definition is fully satisfactory" (Garner, 1995, p. 503). However, a *legal system* "is a procedure

DOI: 10.4324/9781003203155-2

or process for interpreting and enforcing the law" (Cornell Law School, 2020), whatever the law may be. As will be discussed in more detail in "Law, archives, and colonialism," *infra*, the legal systems in this study, descended from various legal systems that differ in how they prioritize different sources of law, and in how they interpret and enforce the law. Knowing the system in which one operates, what sources of law it uses, and how it interprets and accords weight to those sources, is critical.

However, while ARM professionals must attend to the law as it is, it must be stated from the outset that the law is deeply problematic. The imposition of foreign legal systems "through colonialism, conquest, and some might add, neo-colonialism . . . created patterns of power, philosophy, and conduct, whose persistence has been aptly described as the coloniality of power" (Diala and Kangwa, 2019, pp. 190–191). Law's power is such that "colonial legal transplant in Africa was a comprehensive, self-replicating phenomenon, which was accompanied by radical socioeconomic changes that irrevocably affected the education, philosophy, religion, work, food, and dressing of Africans" (Diala and Kangwa, 2019, p. 190); the impact on recordkeeping is no less.

Legal systems which combine elements from multiple legal systems are referred to as "mixed legal systems," although there is disagreement among legal scholars as to precisely which systems are mixed. Perhaps unsurprisingly, scholarship on mixed legal systems originally centred on the mixing of European, and specifically English, common law and Roman civil law systems.

> Scholars in the "mixed jurisdiction" tradition, who follow the footsteps of early British comparatists . . . tend to restrict its scope to a single kind of hybrid where the most comparative research has been done – mixtures of common law and civil law. In that perspective the number of mixed systems in the field shrinks to fewer than twenty around the world. However, many scholars under the influence of legal pluralism . . . use a more expansive, factually oriented definition that enlarges the field and has no obvious limits.
>
> (Palmer, 2012, pp. 368–369)

Even in the narrowest – most Eurocentric – definition, many scholars consider Zimbabwe, South Africa, and Botswana as having mixed legal systems,[2] as their systems combine English common law and Roman-Dutch civil law. This developed due to the three countries' shared colonial history. Roman-Dutch law was introduced into the Dutch Cape Colony (which later became the Cape Colony) in 1652; therefore, Roman-Dutch law was received "directly" in South Africa, although English common law was

significantly mixed. South Africa's law – and thus, the mixed system of civil and common law – was indirectly received into Botswana. The High Commissioners that the British had installed over Bechuanaland (now Botswana) and Southern Rhodesia (now Zimbabwe), which were often governed "by extending Proclamations designed for what is now South African to Botswana. The reception of the mixed system came through the High Commissioner's Proclamation of 10 June 1891," (Fombad, 2010, p. 6). These histories mean that, although all three countries have "mixed legal systems," each has developed uniquely.

As Fombad explains

> [w]hilst the reception of the common law and the civil law in South Africa can be described as direct it was only indirect in the other countries in the region, namely the former three High Commission Territories of Botswana, Lesotho and Swaziland, as well as Namibia and Zimbabwe . . . this reception . . . has influenced and continues to influence the quantum of each element of the mix that was received [and] also affects the way the different legal systems have evolved.
>
> (2010, p. 4)

Scholars estimate that there are fewer than 20 such mixed legal systems in the world (Palmer, 2012). However, as the legal pluralists correctly note, this Eurocentric view falsely posits that the world of laws is a "binary civil law/common law world" (Palmer, 2012, p. 378), when in reality, all legal systems "may be described as diversified blends." Understanding the elements of the legal system in which they work equips ARM professionals to navigate complex, often contradictory, landscapes of compliance, risk, and values. All four countries studied in this case have at least elements of common law, customary law, and indigenous law. Kenya, which arguably has the most clear-cut legal system of the four nations, nonetheless combines common law, customary and indigenous law, and Islamic law as reflected in Table 1.1.

Table 1.1 Mixed law systems

COUNTRY	*MIXED LEGAL SYSTEM*
Botswana	Civil law, customary law, and common law
Kenya	Common law, Muslim law, and customary law
South Africa	Civil law, customary law, and common law
Zimbabwe	Civil law, common law, and customary law

Source: (Palmer, 2012, pp. 379–382)

In the case of South Africa and Botswana, the legacy of multiple colonizers is a system that mixes common law, civil law, customary law, and indigenous law. South Africa and Botswana are, from even the most Eurocentric perspective, mixed law countries, because their legal systems inherited elements from both English common law and Roman-Dutch civil law, although, in reality, both countries' systems include elements of common, civil, customary, and indigenous law. Malila (2010, p. 71) notes that "Botswana, like other post-colonial transitional societies, is still faced with the continuing task of reconciling plural legal systems inherited from the formal colonial power at institutional, process, and value levels." South Africa has a "mixed legal system of predominantly English commercial and public law and Roman-Dutch private law, pervaded by the constitutional principles of personal freedom and the rule of law" (Van der Merwe, 2012, p. 113). As discussed in greater detail in "Case law," *infra*, English common law is a body of judge-made law in which previous cases on an issue are binding on future courts deciding the same issue. It should be noted, however, that common law jurisdictions still employ statutes to regulate their societies. Civil law jurisdictions, on the other hand, place primacy upon codes – the "Roman" in Roman-Dutch refers to the Justinian Code, which forms the basis of European civil law. In civil law systems, case law does not serve as a binding precedent for future cases.

Van der Merwe's (2012) explanation of South African law also raises the important distinction between *public* and *private* law. Public law is that which regulates relationships between individuals and the state, and includes criminal, constitutional, and administrative law. Private law, by contrast, regulates relationships between individuals, and includes contract and tort law. Confusingly, some common law jurisdictions such as the United States and Canada refer to private law as "civil law." Therefore, in South Africa, commerce and relationships between the individual and the state are primarily controlled and can be changed by judge-made law, while the relationships between private individuals are still primarily controlled by legal codes. Within private law, a further category of *personal law* exists, which is "the law that governs a given person in family matters" (Garner, 1995, p. 655). As Palmer (2012, p. 377) writes, "Rarely has any people willingly given up its own personal law or voluntarily accepted someone else's," and it's in the area of personal law where "customary law" is most often recognized. Thus, personal law is the legal area in which precolonial culture and practice are most likely to persist, and records related to personal law may provide a more representative picture of a nation and its peoples.

Zimbabwe faces unusual challenges in the regulation of its records management due to its unique colonial history (Ncube, 2016). Like many colonized nations, Zimbabwe has oral indigenous recordkeeping traditions that

were at odds with the written traditions of settler recordkeeping and government (Chaterera, 2016). However, Zimbabwe, unlike many other nations, was not a full British colony, but was rather under the rule of the British South Africa Company; its rule by a private company meant that its records throughout the colonial period did not belong to the government (either of Zimbabwe or of the United Kingdom), but to a private company based in London. The governmental – and public records – context and challenges in Zimbabwe have largely been in response to the country's struggles with the legacies of colonization.

All four of the nations in this study, continue to bear the marks of colonialism in their legal and bureaucratic systems. Thus, while ARM professionals in Botswana, Kenya, South Africa, and Zimbabwe share issues with archivists in Belgium and Canada, such as custody and control over digital, and especially cloud-based records, they also face challenges that are unique to their contexts. Furthermore, solutions developed for Western nations facing novel records-related challenges, such as data-mining – including access to information and data protection laws – may be inadequate or ill-suited for recordkeeping in Africa. For example, with regard to access to information, the dominant scholarly narrative focuses on legislation as the "solution" to the problem of information accessibility and transparency. This narrative paints African countries and recordkeepers as "failed," without examining the "political, social, administrative, and economic conditions that prevail" (Calland and Diallo, 2013, p. 2) in those countries. Similarly, the legalistic approach that treats data protection laws as the solution to massive data collection and surveillance fails to recognize the colonial socioeconomic dimensions and power disparities ("digital colonialism") at play when Western technology companies extract and exploit data from African people (Coleman, 2019).

Given the mixed nature of the legal systems, there are four primary sources of law in the countries under study: constitutions, statutes and regulations, case law, and customary and indigenous law.

Sources of law

Constitution

"Constitutionalism is the idea that governmental authority is conferred and defined by the people through a fundamental law known as the Constitution" (Diala and Kangwa, 2019, p. 189). A constitution, "a written document containing the principles of governmental organization of a nation" (Garner, 1995, p. 208), is the "supreme law in a country to which all other laws must adhere" (Clegg et al., 2016, p. 2). This means that any proposed (or even passed) law that contradicts the constitution is *unconstitutional*, and therefore

unlawful. As will be discussed in greater detail *infra*, a number of the major themes in the law impacting ARM work are embedded in countries' constitutions. For example, both Botswana and South Africa have a constitutional right of access to information (Adeleke, 2013). However, scholars such as Darch (2013), Diala and Kangwa (2019), and Khan (2020) argue that constitutionalism is deeply problematic in post-colonial states in Africa.

Statutes and regulations

A statute is "a legislative act that the state gives the force of law" (Garner, 1995, p. 829). Statutes are often called "laws" in the lay vernacular. Statutes obtain their authority from the constitution, which "authorizes the legislature to enact it" (Clegg et al., 2016, p. 9). In some countries, such as Kenya, the constitution will divide law-making authority between different legislatures, such as the national and county governments. Regulations, in turn, "are issued under the authority of a statute by a division of the government or by a special body" (Clegg et al., 2016, p. 2). Most of the laws dealt with in this chapter are *omnibus* laws, or laws that address an issue regardless of sector. However, ARM professionals must also be aware of the *sectoral* laws that may apply to their organization, for example, banking laws that impose particular information security requirements or health care laws that impose specific privacy requirements.

Case law

In a number of countries, especially those previous colonized by England, *case law*, or the body of law made up of judicial decisions, is an important source of law. Such systems, called common law systems, treat judgments as one of the most important sources of binding the law under the doctrine of precedent, called *stare decisis*, which means "let decided things stand" (Garner, 1995, p. 825). Under *stare decisis*, court decisions become *precedent* and bind the court in future cases on the same matter. Thus, in a common law system, if the interpretation or application of a particular law is in dispute, it is brought before a court with jurisdiction over the matter. Once that court makes a decision (for example, if the court holds that the Public Officer Ethics Act applies to government archivists and records managers), that decision applies to all future decisions in that court and all courts beneath it. A court may only make decisions on cases that fall within that court's jurisdiction; jurisdiction can be limited either geographically or functionally.

Jurisdiction is given in the constitution and other legislation. Thus, the Supreme Court of Kenya, for example, has jurisdiction geographically over the whole of Kenya; it also has appellate jurisdiction over all disputes

being brought up from the Court of Appeal (see Figure 1.1 for Kenya's court structure). The Supreme Court also has original jurisdiction over disputes concerning presidential elections, which means that disputes concerning presidential elections are initially brought before the Supreme Court, as opposed to being brought up on appeal. Most cases, however, will begin somewhere near the bottom of the hierarchy, and be "brought up" to higher levels of court through the appellate process.

Thus, a decision by the Supreme Court will be binding upon all courts of lower jurisdiction. On the other hand, a decision by the High Court is *not* binding on the Court of Appeal or the Supreme Court, because the High Court is a lower court. Thus, a particular question will (in most cases), be brought before a low-level court (such as a Magistrate Court). If that court's decision is not appealed, it will stand as a binding decision for that court.

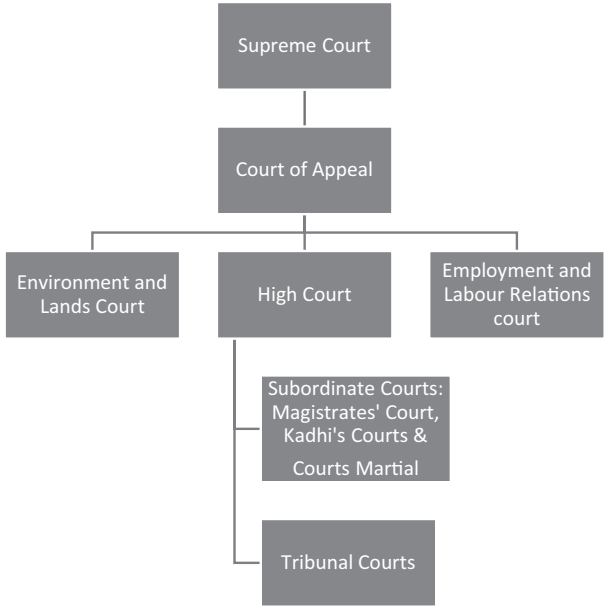

Figure 1.1 Kenya's court structure

Long Description: Figure showing Kenya's courts in hierarchical order. Supreme Court at the top, Court of Appeal below it, High Court below it with Environmental and Lands Court as well as Employment and Labour Relations Courts at the same level. Below the High Court are Subordinate Courts i.e. Magistrates' Court, Kadhi's Courts and Courts Martial. Below subordinate courts are Tribunal Courts

Source: (Kenya Judiciary, 2021)

If it is appealed up to the High Court, the High Court's decision will be binding on the High Court *and* the lower-level courts (i.e., the Magistrate Courts) in the future. As an example, the High Court held in *High Court of Kenya Petition No. 43 of 2012, Famy Care Limited vs. Public Procurement Administrative Review Board & Another [2012]* that "1) The right to information is only enjoyable by Kenyan Citizens, and not foreign citizens [and] **2)** The right to information is enjoyable by **natural Kenya Citizens** and not **Kenyan juridical persons** such as corporations, or associations" (Georgiadis, 2012 emphasis in original). This holding could be overturned by a superior court (the Court of Appeal or the Supreme Court) or by the High Court in a later case. It could also be overturned by legislation (for example, the Access to Information Act could have stated that it applied the right of access to all citizens, natural and juridical, or to all persons, citizen and non-citizen). Unless and until the holding is overturned, however, it is considered "good law" and binding on the High Court and all lower courts.

Furthermore, a decision even by the highest court of Zimbabwe, the Supreme Court, is not binding on any court in Kenya, because Zimbabwe's courts (and legislature) have no jurisdiction over Kenya. However, decisions from a court without binding authority may be used as *persuasive* precedent, one that courts are not obligated to follow, but may consider. Binding precedent is one of the distinguishing characteristics of a common law system; precedent in civil law systems is only persuasive.

Customary law and indigenous law

Finally, it would be remiss to discuss sources of law without discussing customary law and indigenous law, which are related but far from the same thing. *Customary law* is defined as:

> Practices and beliefs that are so vital and intrinsic a part of a social and economic system that they are treated as if they were laws. *Customary law* is handed down for many generations as unwritten law, though it is usually collected finally in a written code.
>
> (Garner, 1995, p. 241)

Diala and Kangwa (2019), however, make the important point that "customary law" in African nations is not the indigenous law that existed prior to colonization. As they explain, "indigenous laws are oral precolonial norms which people observe in their ancient forms, while customary laws are adaptations of precolonial norms to socioeconomic changes" (Diala and Kangwa, 2019, p. 197). Furthermore, "most indigenous laws have transformed into customary laws through people's adaptations to legal,

economic, religious, and globalisation-fuelled changes in intersecting social fields" (Diala and Kangwa, 2019, p. 189). Given the immense dislocations in socioeconomic life imposed by both colonialism and industrial capitalism, Diala and Kangwa (2019, p. 200) argue that adhering to the letter of indigenous laws would be problematic, for the laws existed to uphold community values in a particular context, and "would have changed with or without the influence of colonial rules."

Islamic law

As noted *supra*, Kenya has an additional source of law, Islamic law (*shariah*), which governs some questions of personal law among Muslim Kenyans through courts known as Kadhi's courts. This is also a legacy of colonization. In the late 19th century, when Kenya and other parts of East Africa were placed under either British or German protection, there was a treaty between the Europeans and the Sultan of Zanzibar – the previous sovereign – to have the coastal strip of Tanzania and Kenya respect the Islamic judicial system (Chesworth, 2010). "The colonial administration set up a tri-partite legal system: common law (colonial) courts, Kadhi's courts, and customary courts," (Wario, 2013, p. 153). As can be seen from the chart in Figure 1.1, the Khadi's courts remain subordinate to the common law courts (Supreme Court, Court of Appeal, and High Court of Kenya). The Khadi's courts have limited jurisdiction, being restricted by the Constitution of Kenya to "determination of questions of Muslim law relating to personal status, marriage, divorce and inheritance in proceedings in which all the parties profess the Muslim religion and submit to the jurisdiction of the Kadhi's courts" (Republic of Kenya, 2010, Article 170, Section 5). Although the Khadi's courts existed in the Coastal Strip "much earlier than the period of establishment of British colonization" (Wario, 2013, p. 153), the imposition of the colony extended to the courts beyond the Coastal Strip and the lands subject to the rule of the Sultanate of Zanzibar. The status of the Kadhi's courts was an important point of debate in the adoption of the new constitution, with "debates about the courts . . . embroiled in discussing earlier protracted clashes over resources such as land, economic opportunities, political leadership, and conflicts over control of educational institutions and boundary disputes" (Wario, 2013, p. 164). For recordkeepers in Kenya, questions of Islamic law are likely to arise only in the context of records related to personal law, for example, matters of marriage, divorce, and inheritance (Osiro, 2013). As Wario (2013, p. 157) rightly reminds us, "conflict, or the lack of it, is usually shaped by historical and socio-economic circumstances." Understanding the law of recordkeeping in Africa necessitates tracing several sources of laws that arose in a great

diversity of historical and socio-economic circumstances. For ARM professionals, analysis of both the letter and the spirit of the law may help in the resolution of tricky cases, weighing up what must be done in the name of compliance versus what can or should be done in furtherance of the institution and/or the profession's values.

Hierarchy of laws

It should also be noted that laws are hierarchical – they apply as long as they do not conflict with a law of higher precedence. The broad rights and principles in the Constitution are implemented through statutes, which, in turn, are fleshed out through regulations, and regulations are put into practice through policies and standards. Therefore, in the context of South Africa, the National Archives Act is only valid law if it does not conflict with the Constitution, and the National Archives Regulations are valid law if they do not conflict with either the National Archives Act or the Constitution. There are also a number of government publications (such as the National Archive's Records Management Policy Manual and Advisory Publications) which do *not* have the force of law but could be offered as evidence of the correct interpretation of a law. In the illustration in Figure 1.2, blue sources are law and red sources are not.

Attention must also be paid to the language of the laws themselves – an act will often explicitly state its relationship to other acts. For example, in Kenya, the Access to Information Act (No. 31 of 2016) states that "Nothing in this Act shall limit the requirement imposed under this Act or any other written law on a public entity or a private body to disclose information" (Section 4(5)); thus, disclosure requirements in other legislation, such as the

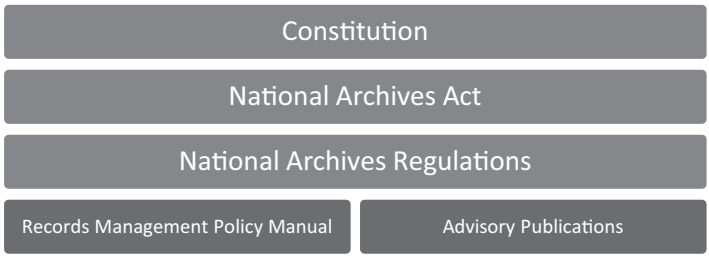

Figure 1.2 Hierarchy of laws

Long Description: Graph showing hierarchy of laws with the Constitution at the top, then the National Archives Act, National Archives regulations and below that two sets of regulations at the same level: Records Management Policy Manual and Advisory Publications

Companies Act, Cap. 486, should not be limited by the Access to Information Act, even if the Access to Information Act would seem to imply otherwise. Sometimes, however, the law does not explicitly address conflicts between acts. Where acts contradict each other, a prudent approach is to adhere to the act with the higher standard until such a time as the conflict is brought before the courts to be resolved (thus, if one act prescribes a minimum five-year retention period, whereas another seems to prescribe seven years for the same type of record, the safest course is to retain those records for seven years). Finally, it must be remembered that policies and standards such as the National Policy on Records Management, while very helpful, are not law and can be changed at any time by their creating bodies.

Interpretation and enforcement of law

One of the great challenges in law is interpreting the law. With regard to statutes, there are a number of rules of interpretation that lawyers and judges rely on; however, those rules are also subject to interpretation. Hon. Malcolm Wallis, Judge of the Supreme Court of Appeal of South Africa, writes that when he was in law school,

> The rule, so we were told, was that statutes should be given their literal meaning, but that courts could depart from this if the literal meaning would result in an absurdity. In a country where much of the legislation affecting the population seemed absurd, this was difficult to comprehend, even in those far-off times.
>
> (Wallis, 2019, p. 2)

Perhaps it is unsurprising, then, that Judge Wallis wrote the decision that expanded the rules of statutory interpretation:

> The present state of the law can be expressed as follows: Interpretation is the process of attributing meaning to the words used in a document, be it legislation, some other statutory instrument, or contract, having regard to the context provided by reading the particular provision or provisions in the light of the document as a whole and the circumstances attendant upon its coming into existence. Whatever the nature of the document, consideration must be given to the language used in the light of the ordinary rules of grammar and syntax; the context in which the provision appears; the apparent purpose to which it is directed, and the material known to those responsible for its production. Where more than one meaning is possible each possibility must be weighed in the light of all these factors. The process is objective,

> not subjective. A sensible meaning is to be preferred to one that leads to insensible or unbusiness-like results or undermines the apparent purpose of the document. Judges must be alert to, and guard against, the temptation to substitute what they regard as reasonable, sensible or business-like for the words actually used. To do so in regard to a statute or statutory instrument is to cross the divide between interpretation and legislation; in a contractual context it is to make a contract for the parties other than the one they in fact made. The "inevitable point of departure is in the language of the provision itself", read in context and having regard to the purpose of the provision and the background to the preparation and production of the document.
>
> (Natal Joint Municipal Pension Fund v Endumeni Municipality, 2012 4 SA 593 (SCA), p. 603–4)

In other words, laws should be interpreted according to their *plain language*, taking into account the context in which the language appears, its purpose, and the context of its creation, with a focus on the law itself, and not the outcome that seems most sensible to the interpreter. In the countries in this study, statutory law co-exists with case law, which, for example, may provide clarity on the meaning of the terms or the scope of the law. Thus, an ARM professional looking to adhere to access to information requirements in South Africa would have constitutional, statutory, and case law to consider together, to understand the full scope of their obligations.

Law, archives, and colonialism

The law-archives interface in the four countries studied has been indelibly shaped by colonialism and by European legal imperialism. As Khan (2020, p. 1) writes, "Colonialism constructed legal identities and subjects, many of which found their way into post-independence constitutional frameworks [. . . leading] to the legacy of colonisation continuing." Katuu (2020, p. 276), discussing the challenges facing ARM professionals in Africa, reminds us that,

> Tracing of different nations throughout the course of the colonial and post-colonial periods is critical in setting the stage for any discussions on current developments. . . . The socio-political history of any nation has a huge impact on the juridical and administrative structure, which forms the overriding context within which ARM professions have to work.

Part of the legacy of colonialism is that the legal systems of previously colonized countries often contain elements of the legal systems of multiple colonizers. Based on their unique pre-colonial, colonial, and post-colonial

histories, each of the countries under study have developed a legal system combining different systems, including customary law, indigenous law, English common law, Roman-Dutch civil law, and, in the case of Kenya, Islamic law, see, for example (Palmer, 2012). Just as colonizers imposed different legal traditions, they also imposed different recordkeeping traditions; speaking of the English and French, Katuu (2020, p. 279) notes that "the recordkeeping traditions from the two major colonial powers on the continent were very different." Furthermore, as discussed in greater detail in the section on customary law, *supra*, each of the countries studied is home to a number of people and cultures who had their own legal systems, cultural values, and norms prior to colonization. European systems of law and records as well as archives were not written on a blank slate, but "coercively changed the normative behaviours of Africans. . . [leading to the creation of customary law that] occurred in the context of dissonance between indigenous and state laws" (Diala and Kangwa, 2019, p. 190). Thus, ARM professionals in the countries studied must function in what may be termed as mixed legal systems which impose unique challenges as noted earlier in this chapter.

National archives and archives law

All four of the countries in this study have National Archives, a national archives law, and other laws directly on the issue of recordkeeping. Even for ARM professionals outside the national archives, the national archives law can provide insight into such matters as how the country's law views the evidentiary character of records, the nature of the country's approach to digital records, and how the country draws the boundary between public and private records.

Botswana

The Botswana National Archives and Records Services (BNARS) was established in 1967 and is governed by the National Archives and Records Services (NARS) Act of 1978 as amended in 2007. Before this Act was enacted, the Botswana National Archives operated through a presidential directive (Mosweu and Simon, 2018, p. 72). The NARS Act provides that:

> The functions of the National Archives and Records Services shall be –
>
> (a) To provide records and information management service to government agencies; and
> (b) To collect, preserve, and access the nation's documentary heritage.
>
> (Botswana, 1978 Section 3A)

However, neither the statute nor its attendant regulations further address electronic records directly, which goes against the assertion that "it is advisable to make clear that the law applies to archival documents irrespective of their physical forms" (Mosweu and Simon, 2018, p. 87). Legislation does not exist in a vacuum; the Electronic Evidence (Records) Act (No. 13 of 2014) and Electronic Communications and Transactions Act (No. 14 of 2014) further support the treatment of electronic records as legally authentic records and provide some guidance as to what is necessary to ensure the ongoing availability and trustworthiness of electronic records (Botswana, 2014a, 2014b). The Electronic Records (Evidence) Act (No. 13 of 2014) and Electronic Communications and Transactions Act (No. 14 of 2014) work together to provide for the legal admissibility and authenticity of electronic records and to facilitate electronic transactions. "Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record" (Botswana, 2014b Section 5(1)). Furthermore, the Electronic Records (Evidence) Act states that "evidence may be presented in respect of any standard, procedure, usage, or practice concerning the matter in which the electronic records are to be recorded or stored," opening the door for consideration of electronic recordkeeping standards (Botswana, 2014b ss. 10).

The *Electronic Communications and Transactions Ac*t gives legal recognition to electronic communications outside the confines of evidence law. "Subject to the provisions of this Act, information shall not be denied legal effect, validity, or enforcement solely on the grounds that (a) it is in the form of an electronic communication" (Botswana, 2014a ss. 3). The Act also states that an electronic writing is sufficient to meet a legal requirement to give information in writing (Botswana, 2014a ss. 4). The Act also provides that retention of electronic records is sufficient to meet legal retention obligations (Botswana, 2014a ss. 9), and that secure electronic signatures are sufficient for notarization and/or verification requirements (Botswana, 2014a ss. 11). When read in the context of these two acts, one can discern a framework for the authorized use of electronic records, even if the archival legislation does not expressly provide for it.

Kenya

The laws addressing archives and records management in Kenya are numerous and diverse. For example, while one would not typically think of the penal code when considering recordkeeping, Cap. 63, Sec. 133 imposes criminal penalties for anyone who destroys or even "fails to preserve" any document that falls within a broad swath of "statutory documents" without the authority to do. While it is beyond the scope of this

chapter to discuss all the laws that regulate recordkeeping, it does try to address the major laws (the Constitution, National Archives Act, and the freedom of information, data protection, and information security laws) that address all public sector recordkeeping. This chapter also does not address county level law. While it is possible that some county level law addresses records management within the areas of power assigned to the counties under Schedule Four of the Constitution, such application would be limited to that particular subject matter within that particular county – the law in Mombasa regarding required records in a childcare facility may well differ from those of Kwale. However, Kenya's government is strongly central; all powers not specifically devolved to the counties in the Constitution belong to the national government, and the national government may regulate within those areas devolved to the counties through an Act of Parliament.

Kenya's national archival law is the *Public Archives and Documentation Service Act*, Cap. 19 (Act No. 2 of 1990). This Act requires that there be "established, constituted and maintained a public department to be known as the Kenya National Archives and Documentation Service" (Section 3(1)), and places upon the director of that service the responsibility for "proper housing, control, and preservation of all public archives and public records" (Section 3(2)). Public archives are defined as "all public records and other records which are housed or preserved in the national archives or which are deemed to be part of the public archives" (Section 2). Public records are defined in the Schedule, Section 2:

1 The records of any Ministry or Government Department and of any commission, office, board or other body or establishment under the government or established by or under an Act of Parliament: Provided that nothing referred to in this paragraph shall include the records of the public trustee or of the registrar-general relating to individual trusts or estates.
2 The records of the High Court and of any other court or tribunal.
3 The records of Parliament and of the Electoral Commission.
4 The records of any local authority or other authority established for local government purposes.

Thus, those records which fall within the purview of the National Archives and Documentation Service include, but are not limited to, public records. In particular, the director is empowered to acquire "any document, book, record, or other material of any description or historical or other value, or any copy or replica thereof which he considers should be added to the public records" (Section 4(1)(h)). It is also worth noting from the definitions

section that "'records' includes not only written records, but records conveying information by any means whatsoever" (Section 2).

For records managers and other custodians of public records, it is important to note that

> It shall be the duty of every person responsible for, or having the custody of any public records to afford to the Director or any officer of the Service authorized by him reasonable access to such public records and appropriate facilities for the examination and selection thereof, and to comply without any undue delay with any lawful directions given by the Director or such officer concerning the assemblage, safe keeping and preservation of such public records or of the transfer of any such public records to the national archives to form part of the public archives.
>
> (Section 4(2))

Thus, custodians of public records have a significant potential obligation to the National Archives and Documentation Service. The Act also creates several offences for willfully destroying or disposing of, defacing, mutilating, or damaging public archives (those records that have passed the archival threshold into the national archives), except in such cases where the director has authorized such destruction (Section 8).

Records in the custody of the public archives are accorded all legal respect. In such cases where public records are required to be kept in or produced from legal custody, they remain in valid legal custody if transferred to the public archives (Section 10). Furthermore, certified copies of records from the public archives are admissible as evidence "in any proceedings" in which the original record would have been admissible (Section 11). Rules for the disposal of records belonging to or being in the custody of the courts or the registrar-general may be made in consultation with the director of the Kenya National Archives and Documentation Service, subject to the provisions of the Public Archives and Documentation Service Act, Cap. 19 (Records Disposal Act, Cap. 14, Section 2).

The Kenya Information and Communications Act, 2009, establishes and empowers the Communications Authority of Kenya to "licence and regulate postal, information and communication services" (Section §5(1)). Part of that broad mandate includes facilitating, promoting, and fostering the development of electronic transactions and commerce (Section 83C). In line with those goals, this act provides for legal recognition of electronic records, stating that,

> Where any law provides that information or other matter shall be in writing then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information

> or matter is – (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.
>
> (Section 83G)

The *Kenya Information and Communications Act*, 2009, provides standards for the retention of electronic records, requiring that:

> Where any law provides that documents, records or information shall be retained for any specific period, then that requirement shall be deemed to have been satisfied where such documents, records or information are retained in electronic form if:
>
> (a) the information contained therein remains accessible so as to be usable for subsequent reference
> (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format that can be demonstrated to represent accurately the information originally generated, sent or received
> (c) the details that will facilitate the identification of the original destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.
>
> (Section 83H)

Under Article 83I, an electronic record is sufficient where the law requires that records or information be retained in their original form, as long as there are adequate safeguards of the integrity and reliability of that record. Article 83P provides for legal recognition of electronic signatures. Article 83S empowers government agencies to utilize electronic records to meet a variety of administrative needs, including delivery of public goods and services, the filing of forms and applications, the issuances of grants and permits, and the receipt of payment.

South Africa

The National Archives and Records Service of South Africa Act (hereafter, National Archives Act or NARS Act) sets out a sophisticated system of archival control and responsibility, anchored in the National Archives and the National Archivist. The Act vests ultimate accountability for "the proper management and care of public records in the custody of governmental bodies," as well as for the non-public record of enduring value, in the National Archivist (Section 13). This Act also empowers the National Archives to promulgate "regulations as to the management and care of public records in

the custody of governmental bodies" (Section 13(3)); such regulations have been issued and provide further detail and direction as to how the National Archives and governmental bodies shall perform functions such as records transfer and disposal, appraisal, and classification. Both the act and regulations have force of law, as far as they do not conflict with the Constitution (or, in the case of the regulations, they do not conflict with the act). The specific accountabilities of the National Archives include all of the traditional archival functions: appraisal and acquisition, arrangement and description, retention and preservation, management and administration, and reference and access. The act and regulations authorize liberal delegation on the part of the National Archivist and leave the National Archives significant liberty in how they meet their responsibilities (for example, the regulations require only that public bodies use an approved classification system; they do not dictate the required classification system). Ultimately, the National Archives Act "provides the anchor for the management of records, including digital records" (Katuu and Ngoepe, 2015, p. 61).

Mosweu and Simon (2018, p. 85) compare Botswana's archival legislation to the National Archives Act, which outlines nine functions of the National Archives. One function which South African legislation makes explicit, as Mosweu and Simon (2018) discuss at some length, is to "collect non-public records with enduring value of national significance which cannot be more appropriately preserved by another institution" (South Africa, 1996 Section 3 (d)). However, while the primary Botswanan legislation does not directly provide for such acquisitions, Part VI: General ss 2728, Section 28 of the National Archives and Records Services Regulations does provide for the donation of such archives, with Schedule 1, Form D of those regulations providing a Deed of Gift for such acquisitions. Furthermore, South Africa's (1996 Chapter 59:04) NARS Act empowers the director of the National Archives to, "on behalf of the government, acquire by purchase, donation, bequest or otherwise any private archive which in the opinion of the director is or is likely to be of enduring or historical value." Thus, the legislation clearly contemplates, even if it does not directly specify, acquisition of private archives as part of the mandate of the National Archives and Records Service. The two functions specified are incredibly broad – they could be summarized as current records management and archives management – and arguably contemplate the narrower functions of the South African legislation within their sweep. The powers given to the director (ss. 5 et seq.) comprise the full range of archival functions, including appraisal and acquisition, arrangement and description, retention and preservation, management and administration, and reference and access. The Minister also has broad powers under the statute to bring records within the purview of the National Archives and Records Service, being empowered to "declare any

public body, corporation, society, association, institution, organization or any body of persons, whether incorporated or not, to be a prescribed body for the purposes of this Act and the documents of such body shall be public records" (South Africa, 1996 Chapter 59:04, ss. 7).

The NARS Act also accords legal authenticity to records within the custody of the National Archives and Records Service, providing:

> A copy of or extract from any record in the National Archives and Records Services or place of deposit purporting to be duly certified as true and authentic by the Director, or by any authorized officer or by the custodian of the public archives in any place of deposit where such record is kept, and authenticated by having impressed thereon the official seal of the National Archives and Records Services or of the place of deposit, shall be admissible in evidence if the original record would have been admissible in evidence in any proceedings.
>
> (South Africa, 1996 Chapter 59:04, ss. 17)

Mosweu and Simon (2018) fairly raise the lack of clarity within the NARS Act regarding electronic records. The statute provides a definition of "records" that clearly intends to include digital as well as paper records:

> **"records"** (emphasis in original) includes any electronic records, manuscript, newspaper, picture, painting, document, register, printed material, book, map, plan, drawing, photograph, negative and positive pictures, photocopy, microfilm, cinematograph film, video tape, magnetic tape, gramophone record or other transcription of language, picture or music, recorded by any means capable of reproduction and regardless of physical form and characteristics.
>
> (South Africa, 1996 Chapter 59:04, ss. 2(c))

Zimbabwe

The National Archives of Zimbabwe was originally established during the 1930s under the colonial government. However, this statement is a vast oversimplification of the complex history of those archives. As noted *supra*, during the colonial period, Zimbabwe was under the rule of the British South Africa Company. Among records being expropriated to London, and those within the country being "not properly cared for and . . . haphazardly destroyed . . . Zimbabwe lost some crucial part of its documentary heritage" (Chaterera, 2016, p. 119). The National Archives of Rhodesia (the country now known as Zimbabwe was "Southern Rhodesia" during the colonial period, while Zambia was "Northern Rhodesia") was created by an Act

of Parliament (the Parliament of the United Kingdom) in 1935. Chaterera (2016, p. 119) explains the subsequent development of and changes in the composition of these archives:

> in 1946 . . . the Southern Rhodesian government archives took responsibility in Northern Rhodesia and Nyasaland [now Malawi] to form what came to be known as the Central African Archives [citation omitted]. In 1953, three Southern African territories named Southern Rhodesia (Zimbabwe), Norther Rhodesia (Zambia) and Nyasaland (Malawi) came together to form a federation that came to be known as the Central African Federation (CAF) . . . which resulted in the Central African Archives changing its name to the National Archives of Rhodesia and Nyasaland and further renamed the National Archives of Rhodesia in 1963 after the federation had dissolved. The name changed to the National Archives of Zimbabwe in 1980 when the country achieved independence.

The National Archives of Zimbabwe, then, are inextricably bound to the colonial history of both Zimbabwe and its neighbouring nations (see Figure 1.3 for predecessor institutions of the national Archives of Zimbabwe).

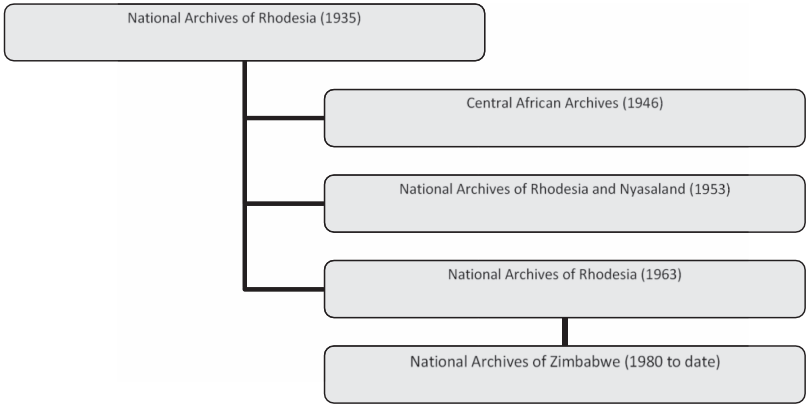

Figure 1.3 Predecessor institutions of the National Archives of Zimbabwe

Long Description: Figure showing archival institutions that preceded the National Archives of Zimbabwe starting from the National Archives of Rhodesia (1935) with relationships with the Central African Archives (1946), National Archives of Rhodesia and Nyasaland (1953), National Archives of Rhodesia (1963) and eventual National Archives of Zimbabwe (from 1980 to date)

Source: (Chaterera, 2016, p. 120)

The National Archives of Zimbabwe Act (Chapter 25:06) provides for the continuity of those archives after the repeal of their creating legislation, "for the storage and preservation of public archives and public records" (Section 3). Public archives are defined as:

> (a) Any public record which –
>
> i Is twenty-five years old; and
> ii Has been specified by the Director as being of enduring or historical value; or
>
> (b) Any other record or material acquired for the National Archives by the Director.
>
> (Section 2)

Public records, in turn, are defined solely based on custody: "public record means any record in the custody of any Ministry" (Section 2). Thus, those records that fall within the purview of the National Archives of Zimbabwe include, but are not limited to, public records. In particular, the director "may acquire by purchase, donation, bequest or otherwise any record or other material which in his opinion is or is likely to be of enduring or historical value" (Section 5(c)). Although the director seemingly has broad powers, he "may, in respect of any Ministry . . . inspect and examine [their] records [and/or] give advice or instructions concerning the filing, maintenance and preservation . . . of [those] records" (Section 6). The director is ultimately limited by the discretion of the Minister responsible for said Ministry, whose decision is final. Similarly, in cases where the director of the National Archives is denied access to records by a local authority, his only recourse is to the relevant Minister, who has ultimate authority to grant or deny such access as s/he/they deem(s) fit. The role of the National Archives of Zimbabwe is largely circumscribed to an advisory role.

Understandably, given the colonial history of Zimbabwe, much of the National Archives Act is concerned with the protection of historical records, and the imposition of penalties upon individuals who would take such records. In the context of broader archival practice, however, the National Archives of Zimbabwe Act is both out of date and stingy in its context and guidance. As Mutsagondo and Chaterera (2016) point out, the Act, having been written in 1986, makes no provision for electronic records. The Act defines "record" broadly enough that electronic records are almost certainly within its purview ("any medium in or on which information is recorded" (Section 2)); however, extraordinarily little guidance is given in the Act itself or in secondary legislation as to what is to be done with and to those records and by whom. As Ngoepe and Saurombe (2016, p. 37) put it, "Zimbabwe

does not have archival legislation that specifically caters for the creation, use, maintenance and disposal of electronic records, which has resulted in records management practitioners resorting to a hit-or-miss approach when managing electronic records." Mutsagondo and Chaterera's (2016) survey of records managers working under the Act revealed that such critical areas as records transfer, destruction, authenticity, capacity, and appraisal are all negatively impacted by the lack of legal guidance concerning electronic records. The Act also lacks provisions commonly found in archival laws, such as those providing for the legal authenticity of certified copies of records provided by the archives (be they paper or electronic). While the Act is broad and flexible, and, therefore, could be updated through secondary legislation, there has been no attempt to do so thus far.

> The current legal set-up does not guarantee the controlled management of electronic records throughout their lifecycle, and this potentially robs the country of its documentary heritage. In such circumstances, the country may find it difficult to plan for its present and its future.
>
> (Mutsagondo and Chaterera, 2016, p. 255)

In all four countries, the national archives and their animating law(s) are a product of the broader legal system, the socioeconomic realities within the country, and the technical and political needs that the archival system serves. As challenging as it may prove with the many other demands upon them, ARM professionals should always remain conscientious as to whom their institutions serve, even if the law is neutral on its face as to which citizens' records it will preserve. As Bhebhe and Ngoepe (2021, p. 156) found in the cases of both Zimbabwe and South Africa, even after liberation from colonization, the national archives – like archives worldwide – are largely controlled by elites who "have shaped the national historical narrative into their favour and to the detriment of the minority groups whose stories have been silenced, distorted, manipulated and obliterated in some cases."

Access to information

Access to information (ATI) laws, also known as right to information (RTI) laws or freedom of information (FOI) laws, reflect the general view that access to information is a fundamental human right. Indeed, Article 9 of the African Charter on Human and Peoples' Rights provides that, "1. Every individual shall have the right to receive information. [and] 2. Every individual shall have the right to express and disseminate his opinions within the law" (Organisation of African Unity, 1981). In its "Declaration of Principles on Freedom of Expression and Access to Information in Africa," the African

Commission on Human and Peoples' Rights (2019, p. 3) declares that "The respect, protection and fulfilment of these rights is crucial and indispensable for the free development of the human person, the creation and nurturing of democratic societies and for enabling the exercise of other rights."

Since the 1980s, regional and international organizations have applied both direct and indirect pressure on the tenets of transparency, good governance, and accountability in public sector reform initiatives globally. Other African examples include the Declaration of Principles on Freedom of Expression in Africa (African Commission on Human and Peoples' Rights, 2002), the African Charter on Democracy, Elections, and Good Governance (African Union, 2007), and the Model Law on Access to Information for Africa (African Commission on Human and People's Rights, 2013). These efforts underpinned the passage of ATI legislation or constitutional provisions in a number of countries from the 1990s through the 2010s (Lemieux and Trapnell, 2016, p. 14). There are two trends in the enactment of ATI in Africa. First, some countries have enacted fully-fledged legislation, often accompanied by implementation regulations. These include South Africa and Zimbabwe in 2002, Uganda in 2005, Liberia and Guinea in 2010, Nigeria in 2011, Cote d'Ivoire and Rwanda in 2013, Burkina Faso in 2015, and Kenya, Malawi, Tanzania, and Tunisia in 2016 (Katuu, 2011; Right2Info, 2021). Secondly, some countries only have a constitutional provision. These include Mozambique in 1990, Ghana and Madagascar in 1992, Seychelles in 1993, Ethiopia in 1994, Guinea Bissau in 1996, Senegal in 2001, Angola in 2002, Democratic Republic of Congo in 2006, and Cape Verde in 2010 (Right2Info, 2021).

ATI laws have been embraced worldwide as "part of the overall global trend toward more transparent and open government" (Lemieux and Trapnell, 2016, p. 1). ATI laws are supposed to

> improv[e] the efficiency of the government and increase[e] the transparency of its functioning by:
>
> - Regularly and reliably providing government documents to the public
> - Educating the public on the significance of transparent government [and]
> - Facilitating appropriate and relevant use of information in people's lives.
>
> (Lemieux and Trapnell, 2016, p. 1)

However, "the ATI debate [globally] has been mostly articulated in terms of 'advances' by legislation . . . this juridical approach to ATI has embedded in it an ideological dimension. . . . the common normative view of diffusion of

ATI is based on an acceptance of liberal values, within the broader context of human rights discourse" (Calland and Diallo, 2013, p. 2). This juridical viewpoint is inescapably embedded in Western values, including constitutionalism and an individualistic approach to rights. Furthermore, as can be seen in this study, mere implementation of ATI laws is no guarantee that information will actually be made available. Indeed, in the case of Zimbabwe, the primary ATI law has been used to suppress and control information that is unfavourable to the government. Thus, ATI laws are far from a panacea. Nonetheless, ARM professionals must understand the obligations that such laws impose and their impact on the transparency and accountability functions of records and archives, as well as their potential to positively impact recordkeeping (Shepherd et al., 2011).

Botswana

Unlike the other countries in this study, Botswana does not have legislation providing for access to information or freedom of information. Khumalo et al. (2016, p. 113) state that the closest to a public right of access to government-held information is Section 12 of the Constitution, which states:

> Except with his or her own consent, no person shall be hindered in the enjoyment of his or her freedom of expression, that is to say, freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his or her correspondence.
>
> (Constitution of Botswana, 1966, Section 12)

However, as noted by Khumalo et al. (2016, p. 114), this is a "passive provision for access to information" which provides only "freedom to receive information. . . [and not] to seek information from the government." Botswana's legal framework skews heavily in favour of government secrecy; public officers within the National Archives and Records Services must make an oath of declaration of secrecy (Botswana, 1978 Chapter 59:04, ss9). Indeed, Balule and Dambe (2018, p. 431) go so far as to assert that "openness and transparency are alien concepts in Botswana's democracy," noting that public servants who reveal "any information coming to their knowledge or the nature or content of any documented communicated to them either in the course of their duty or by virtue of their employment [are subject to] summary dismissal" (*Id*.). Disclosure requires permission of the Permanent Secretary of the public servant's ministry (*Id*.).

A number of laws in Botswana, including the National Security Act (Chapter 23 of 1986, amended in 2005), the Cybercrime and Computer Related Crimes Act (Chapter 08:06), the Media Practitioners Act (Act 29 of 2008), and the Intelligence and Security Services Act (Chapter 23:02), strongly favour secrecy over openness. Furthermore, the dimensions of the constitutional right to freedom of information have not been defined.

> After half a century since the adoption of the Constitution, it is perhaps surprising that, given the importance of the right of access to information, and the difficulties faced by individuals in accessing State-held information, courts of law in the country have not yet been called upon to make a determination on the ambit of the right of access to information guaranteed in the Constitution.
>
> (Balule and Dambe, 2018)

There seems to be no movement towards increasing access to information through law or policy (Khumalo et al., 2016).

Kenya

Article 35 of the Constitution of Kenya guarantees both access to information and the right to be forgotten, stating:

> (1) Every citizen has the right of access to –
>
> (a) information held by the State; and
> (b) information held by another person and required for the exercise or protection of any right or fundamental freedom.
>
> (2) Every person has the right to the correction or deletion of untrue or misleading information that affects the person.
> (3) The State shall publish and publicise any important information affecting the nation.
>
> (Constitution of Kenya, 2010, Article 35)

How those rights are to be exercised and their limits are further defined in relevant legislation, in particular, the *Access to Information Act*. As Abuya (2013, p. 219) notes, however, this right, which is available to Kenyan citizens only, is subject to Article 24 of the Constitution, which provides that the right of ATI can be limited by "to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom." Magina (2019, p. 87), in a study examining why Kenyans struggle to access information after the passage of the *Access to Information Act*, identifies the limitation of the right to citizens as "[t]he major limitation of the right of access."

The *Access to Information Act* (Act No. 31 of 2016) is meant to fulfil a number of accountability and transparency goals by providing access to records and other forms of information. The definition of "information" given in the act is extensive, including "all records held by a public entity or a private body, regardless of the form in which the information is stored, its source or the date of production" (Section 2). The inclusion of private bodies is particularly notable; ATI laws often focus only on public bodies.

The legislative purpose of the *Access to Information Act* is to:

> (a) give effect to the right of access to information by citizens as provided under Article 35 of the Constitution;
> (b) provide a framework for public entities and private bodies to proactively disclose information that they hold and to provide information on request in line with the constitutional principles;
> (c) provide a framework to facilitate access to information held by private bodies in compliance with any right protected by the Constitution and any other law;
> (d) promote routine and systematic information disclosure by public entities and private bodies on constitutional principles relating to accountability, transparency and public participation and access to information;
> (e) provide for the protection of persons who disclose information of public interest in good faith; and
> (f) provide a framework to facilitate public education on the right to access information under this Act.
>
> (Access to Information Act, 2016, Section 3)

Kenya's *Access to Information Act* is notable as compared to similar legislation in a number of other jurisdictions for its twin focus on providing access to both public entity and private entity information, in such cases where a private entity either "receives public resources and benefits, utilizes public funds, engages in public functions, provides public service as exclusive contracts to exploit natural resources" (Access to Information Act, 2016, Section 2) or

> is in possession of information which is of significant public interest due to its relation to the protection of human rights, the environment or public health and safety, or to exposure of corruption or illegal actions or where the release of the information may assist in exercising or protecting any right.
>
> (Access to Information Act, 2016, Section 2)

Kenya's Access to Information Act also provides a far broader right to information than similar legislation in other jurisdictions; under the Act, "every citizen has the right to access to information held by – (a) the State; and (b) another person where that information is required for the exercise or protection of any right or fundamental freedom" (Section 3). However, the use of the word "citizen" in both the Access to Information Act and Article 35 of the Constitution is important; the High Court in High Court of Kenya Petition No. 43 of 2012*, Famy Care Limited vs. Public Procurement Administrative Review Board & Another* (2012) held that the right of access to information embodied in Article 35 of the Constitution is a right only of natural persons who are Kenyan citizens.

Another area in which the Access to Information Act is noticeably broad is in its definition of "personal information." Under the Access to Information Act, "personal information" means information about an identifiable individual, including, but not limited to –

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical, psychological or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
(c) any identifying number, symbol or other particular assigned to the individual;
(d) the fingerprints, blood type, address, telephone or other contact details of the individual;
(e) a person's opinion or views over another person;
(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the o original correspondence;
(g) any information given in support or in relation to an award or grant proposed to be given to another person;
(h) contact details of an individual.

(Access to Information Act, 2016, 2)

The inclusion of "correspondence," which encompasses not just data, but also records, is a notable departure from freedom of information legislation in other jurisdictions.

In addition to the duty to fulfil information requests, the Access to Information Act imposes several duties upon ARM professions in public entities. Article 17 provides for the "management of records," which are defined as "documents or other sources of information compiled, recorded or stored in

written form or in any other manner and includes electronic records." Section 17(2) requires that public entities:

> keep and maintain –
>
> (a) records that are accurate, authentic, have integrity and useable; and
> (b) its records in a manner which facilitates the right of access to information as provided for in this Act.

Section17(3) imposes a duty on public entities to document and a requirement to digitize.

The duty to document requires that public entities, at a minimum, "create and preserve such records as are necessary to document adequately [the entity's] policies, decisions, procedures, transactions and other activities it undertakes pertinent to the implementation of its mandate" (Section 17(3)(a)). The digitization requirement demands that, "not later than three years from the date from which this Act begins to apply to [a public entity, the entity shall] computerize its records and information management systems" (Section 17(3)(c)).

The *County Governments Act* (No. 17 of 2012), imposes access to information obligations upon government at the county level, stating that one of the principles of citizen participation in county government is "timely access to information, data, documents, and other information relevant or related to policy formulation and implementation" (Section 87(a)). Article 96 provides directly for the right of access to information vis-à-vis county government, stating that:

> Every county government and its agencies shall designate an office for purposes of ensuring access to information as required by subsection (1)(3). Subject to national legislation governing access to information, a county government shall enact legislation to ensure access to information.
>
> (*County Governments Act*, 2012, Art. 96, Sec. 2)

South Africa

Lemieux and Trapnell (2016) characterize South Africa as being in the "middle" range of countries with regard to ATI – those countries that have implemented ATI laws but are still facing challenges. The authors state that: "South Africa has an active human rights commission that conducts regular evaluations and training for civil servants but lacks enforcement authority and faces the challenge of low capacity within the civil service" (Lemieux and Trapnell, 2016, p. 4). South Africa's ATI law is the *Promotion of Access to Information Act* (No. 2 of 2000, hereinafter PAIA). PAIA, which finds its analogue in other jurisdictions' freedom of information legislation, makes meaningful the promise of access to information in Section 32 of the Constitution.

PAIA explicitly overrides all limitations on the disclosure of records in other legislation if those limitations are in conflict with the purposes or a specific provision of PAIA (Section 5). PAIA sets out guidance for accessing information held by two types of bodies: public bodies and private bodies. The statute places authority for PAIA on both the records holders and the South African Human Rights Commission, which receives the mandatory PAIA manuals from various bodies and provides PAIA guidance. PAIA provides procedural guidance on how to access information held by both public and private bodies, addressing issues including the right of access, manner of access, time limits for response, grounds for refusal, and third-party notice and intervention.

PAIA protects information officers who act in good faith, shielding them from any civil or criminal liability from attempting to discharge their duties under PAIA. However, for the individual who acts in bad faith, this law imposes potential criminal liability:

> A person who with intent to deny a right of access in terms of this Act- (a) destroys, damages or alters a record; (b) conceals a record; or (c) falsifies a record or makes a false record, commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years.
>
> (Section 90(1))

Two major – and, as of the time of writing, unresolved – points of conflict between the National Archives Act and PAIA must be pointed out. The first is a question of responsibility: the National Archives Act gives extensive powers to the National Archives, whereas PAIA centres authority for South Africa's information regime in the Department of Justice and Constitutional Development. The second is a question of records release. The National Archives Act provides that information should be made available automatically after 20 years but gives the National Archivist the authority to make records available sooner. PAIA, by contrast, empowers public bodies to decide, and make known through their manuals, what information is automatically available. These conflicts in the law are not resolved.

Zimbabwe

The Constitution of Zimbabwe Amendment (No. 20 of 2013) guarantees the right of access to information. Section 20 of the Lancaster House Constitution also provides for the "freedom to hold opinions and to receive and impart ideas without interference." Zimbabwe's Access to Information and Protection of Privacy Act (Chapter 10:27) (hereinafter AIPPA) is highly unusual among freedom of information laws. While it provides some of the expected freedom of information provisions, covered in the table law,

significant portions of AIPPA are concerned with restrictions on the publication and dissemination of information by media and journalists. AIPPA also applies only to records in the custody or control of public bodies; Zimbabwe currently does not have any controls on data privacy in the private sector beyond common law torts such as invasion of privacy.

Zimbabwe's Access to Information and Protection of Privacy Act functions primarily in support of the state, rather than citizens. Section 80, "Abuse of journalistic privilege," flips the public interest test commonly found in freedom of information legislation on its head. The public interest test typically weighs in favour of releasing information in order to enhance transparency and improve the ability of citizens to hold government accountable. Section 80 of AIPPA, by contrast, provides that publishing "any statement – (i) threatening the interests of defence, public safety, public order, the economic interests of the State, public morality or public health" (Section 80(1)(c)(i)) is an offence, which can be punished with "imprisonment for a period not exceeding two years" (Section 80(1)). In other words, AIPPA requires that information be withheld whenever its publication goes against the interests of the state.

Manganga (2012, p. 104) asserts that, "legislations like Access to Information and Protection of Privacy Act (AIPPA) and the Public Order and Security Act (POSA) have enabled the government to exert a stranglehold over the media, media houses, and the free flow of information since 2002." Moyo (2013, p. 72) states that "The ZANU PF government since 2003 used the draconian AIPPA to shut down five newspapers including the Daily News, an important daily paper harshly critical of the government."

As Calland and Diallo (2013, p. 6) put it, "few scholars or practitioners would be easily convinced that Zimbabwe's 2002 Access to Information and Privacy Act is anything other an ATI law in name alone, given the oppressive use to which it has been put."

ATI and the ARM profession

As can be seen from the previous analysis, while the right to information is important in the realization of other rights and the promotion of good governance, the effectiveness of ATI laws is a product of the realities on the ground. As Adeleke (2013, p. 83) explains, "the judicial right to information is largely irrelevant as a solution to political problems in authoritarian or undemocratic states," a reality demonstrated by the use of AIPPA as a tool of political oppression in Zimbabwe. Even in countries where ATI rights exist as a matter of law, practical barriers often exist to exercising those rights. Abuya (2013, p. 218), writing about ATI in Kenya prior to the implementation of the *Access to Information Act*, sums up a common experience with ATI throughout the studied countries (and indeed, throughout the world): "although the process seems straightforward in theory, several hurdles are

faced in reality." The ARM profession is critical to reducing those hurdles – only through good recordkeeping can the necessary information be preserved and made accessible. Indeed, "[m]uch of the argument we advance for the recordkeeping imperative hinges around notions of accountability and audit" ensuring that the accountability of government to its citizens, as provided through ATI, is a central mandate of public records managers (Hofman, 2020, p. 219). Even those in private organizations may find themselves subject to ATI requirements, as noticed previously. However, effective ATI requires more than excellent recordkeeping, regardless of the dedication and efforts of ARM professionals. "ATI is an intricate concept, not easily reduced to simple numbers or laws; it requires complex shifts in power relations and bureaucratic culture for it to take root and flourish" (Calland and Diallo, 2013, p. 8).

Data protection

Privacy and, specifically, balancing privacy and access in the face of digital technologies, have become a universal challenge for ARM professionals. As McLeod (2019, p. 18) writes:

> [f]or cloud users one of the challenges to emerge from the InterPARES research was balancing security, privacy, and access, given their various tensions [including] privacy and access to data and records; between what is public and what is private data; between managing organizational risk in a public accountability context and protecting personal information while still making data public; and balancing democratic goals with those for business innovation.

Botswana

Botswana's *Data Protection Act*, *2018* (Act 32 of 2018) has been assented to by Parliament but as of this writing, is not yet in force. The *Data Protection Act* (DPA) is quite modern. As Daigle (2021, p. 14) notes,

> the DPA contains numerous provisions which align with the [European Union's General Data Protection Regulation, the current "gold standard" for data protection], and much of the structure of the law as well as the rights of individuals are very similar to the EU data protection law.

Daigle (2021, p. 14) summarizes some of the major provisions of Botswana's DPA:

> For personal data to be processed legally in Botswana, the consent of the data subject must be gathered (this consent can also be revoked).

> In certain circumstances, this consent will not be required – i.e., if data must be processed in order to complete the terms of a contract to which the data subject is a party, to comply with a legal obligation, to protect the data subject's "vital interests," or to perform an activity in the public interest. Data must also be kept for no longer than necessary, and its processing must have a clearly defined purpose. Moreover, firms must ensure that they have taken appropriate security and technical measures to prevent the theft of personal data (though the law does not define what measures specifically must be taken). Fines for noncompliance can reach as high as 500,000 Botswana pula (approximately $43,000) and can include imprisonment for up to nine years.

The potential punishment for violation of the DPA makes it clear that the legislature intended for this law to "have teeth," or to be enforceable.

Kenya

In Kenya, Article 31 of the Constitution provides for a right of privacy; this right, however, is not absolute. Article 24(1) provides for the limitation of fundamental rights in view of countervailing interests. Kenya's *Data Protection Act* (No. 24 of 2019) is very recent, having come into force in 2019, with regulations promulgated in 2020. Like Botswana's *Data Protection Act*, Kenya's DPA aligns fairly closely to the European Union General Data Protection Regulation (EU GDPR), centering the processing of personal data on principles of consent, transparency, and lawfulness, providing data subjects with a number of rights, and imposing duties on data controllers and processors. Of particular note to ARM professionals is Article 53, which provides exemptions for the processing of data for "historical, statistical or research purposes," which will likely include archives. The DPA also established the Office of the Data Protection Commissioner (www.odpc.go.ke/), which is tasked under Article 8 with overseeing the implementation of the Act, establishing and maintaining a register of data controllers and processors, providing oversight on data processing, and investigating and inspecting data processing operations.

Some further statutes also provide grounds for data privacy claims. Article 31 of the *Kenya Information and Communications Act* (No. 1 of 2009) makes it an offence for telecommunications firms to unlawfully intercept messages from their clients or to disclose such messages, while Article 83 of the same Act makes unauthorized access to a computer system an offence. In the *Banking (Credit Reference Bureau) Regulations*, 2013, Article 49 et seq., data protection measures such as processing limitations, purpose specification, and information quality are imposed, but only upon the small sector of credit reporting. Such data protection mechanisms are not required more broadly.

Informational privacy, including privacy in records, is also undermined by the use of data surveillance by the state security apparatus. Kenya has passed a number of laws enabling data surveillance, including the *National Intelligence Service (NIS) Act*, 2012; the *Security Laws (Amendment) Act*, 2014; and the Prevention of Terrorism Act (2012). This pattern is not unique to Kenya – state security is often the justification for both secrecy and surveillance. Under these laws, fundamental rights – such as privacy and access to information – are limited or even suspended in the pursuit of countervailing state interests. These laws include provisions that directly concern ARM professionals. For example, the National Intelligence Service (NIS) Act (2012), in Article 45, empowers

> an officer of the Service . . . to obtain any information, material, record, document or thing and for that purpose – (a) to enter any place, or obtain access to anything; (b) to search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record document or thing; (c) to monitor communication; or (d) install, maintain or remove anything.

The Security Laws (Amendment) Act (2014) provides explicitly for limiting of the right of privacy, stating that,

> (1) The National Security Organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary. . . . (3) The right to privacy under Article 31 of the Constitution shall be limited under this section for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism.

On the other hand, the security apparatus is also used to deny access to records, including those that are ostensibly public. For example, the Official Secrets Act, Cap. 187 (Act No. 31 of 2016), makes it an offence for anyone who

> obtains, collects, records, publishes or communicates in whatever manner to any other person any code word, plan, article, document or information which is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power or disaffected person.
>
> (Section 3(1)(c))

South Africa

The *Protection of Personal Information Act* (POPI Act) operationalizes the right to privacy in Section 14 of the Constitution. This sophisticated

data protection act, which came into effect in 2020, outlines the rights of data subjects, the obligations, both in terms of rights and security, of data processors, and the mechanisms for enforcement; it applies to the collection, storage, use, dissemination, and deletion of personal information (and thus applies to all recordkeeping and archives that deal with people's individually identifiable information). The statute embodies accepted data protection principles: "The conditions for the lawful processing of personal information by or for a responsible party are the following: [accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation]" (Section 4(1)). Lawful data collection and processing under POPI requires the party responsible for the processing to:

- ensure compliance with the POPI Act;
- not use personal information beyond the purpose for which it was given;
- only process personal information where:
    - the data subject or their surrogate has consented;
    - processing is necessary for a contract to which the data subject is a party;
    - processing complies with an obligation imposed by law on the responsible party;
    - processing protects a legitimate interest of the data subject;
    - processing is necessary for the proper performance of a public law duty by a public body; or
    - processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.
- specify a specific, explicitly defined, and lawful purpose for the collection of personal information.

Of particular concern to ARM professionals is Section 14, "Retention and restriction of records." This section sets out several different retention requirements for records containing personal information:

- Records must be maintained for the minimum time to achieve the purpose for which the information was collected, *unless*
    - the responsible party needs the record for lawful purposes related to its functions or activities;
    - retention is required by a contract between the parties; or
    - the data subject or his/her surrogate consents to longer retention.

- Records may be retained for longer for historical, statistical, or research purposes, as long as there are safeguards to prevent the record being used for other purpose.
- Records *must* be retained when they are used to make a decision about a data subject for a long enough period to give the data subject an opportunity to request access to that record.

Section 14 also requires the responsible part to destroy, delete, or de-identify a record of personal information as soon as possible once the right to retain the record has expired. Pursuant to Section 17, responsible parties must maintain documentation of all processing operations under their responsibility; under Section 19, responsible parties must also secure the integrity and confidentiality of personal information under their control through appropriate security measures. It should also be noted that the regulator may grant exemptions to responsible parties from the requirements of the POPI Act under Sections 37 and 38; Section 37(2)(e) specifically provides for "historical, statistical, or research activity" as a public interest which may justify exemption. The POPI Act also imposes data localization, limiting transborder transfer of personal information to those cases where the receiving jurisdiction has laws providing for the same level of protection as South Africa; the data subject consents to the transfer; the transfer is necessary for the performance of a contract between the data subject and the data processor; the transfer is necessary for the performance of a contract in the interest of the data subject; or the transfer is for the benefit of the data subject and obtaining consent is impracticable, and likely, if it were practicable (Section 72).

However, empirical research has shown a gap between the law's requirements and privacy as practiced in South Africa. Da Veiga (2020, p. 65), reporting on a survey of South Africans, found that "regulatory requirements (in this case, the POPI Act) are perceived as not being met. The results indicate that while consumers in South Africa have a high expectation for privacy, it is not met in practice."

Zimbabwe

Section 57 of the constitution of Zimbabwe guarantees the right of privacy; some of those guarantees are relevant to records in that they address data privacy. The relevant constitutional language states, "Every person has the right to privacy, which includes the right not to have – . . . (d) the privacy of their communications infringed; or (e) their health condition disclosed." As Ncube (2016, p. 105) explains, "There is as yet no reported case law on the interpretation of the new Zimbabwean constitutional provisions. However, as they so closely mirror

South African provisions, it is likely that Zimbabwean courts will be persuaded by South African case law." Van der Bank (2012, p. 79), writing on a South African case covering the privacy provisions of the South African Constitution (*S v Nkabinde* 1998 8 BCLR 996 [N]), writes that, "The entrenchment of the right to privacy in [the Constitution] compels the Government to initiate steps to protect neglected aspects of the right to privacy in South Africa, such as data privacy or the protection of personal information." If, then, the Zimbabwean courts interpret South African cases such as *Nkabinde* as persuasive authority, they might well find that similar provisions in the Zimbabwean constitution also compel the government to protect the right privacy. At this point in time, however, the question remains open. At the time of this writing, Zimbabwe has a cybersecurity and data protection bill that has passed the Senate and is awaiting presidential approval. However, the proffered data protection bill is deeply problematic.

The *Cyber Security and Data Protection Bill*, 2019, has drawn deep criticism, with Transparency International arguing that the bill "will obstruct the crucial role of civil society and the media in the fight against corruption and undermine any recent progress." One section that critics point to is 164B, "Cyber-bullying and harassment." Section 164B provides that

> any person who unlawfully and intentionally by means of a computer or information system generates and sends any data message . . . with the intent to . . . degrade, humiliate or demean the person of another . . . shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not to exceed ten years.
>
> Transparency International (2020)

Critics read this section – not unreasonably – as threatening up to ten years prison for people who use the Internet to criticize political figures. The "data protection" bill does include many of the EU GDPR provisions seen in other data protection bills, such as duties of data controllers and processors. But, by wedding data privacy to cyber security and, particularly, to a cyber-security bill with extensive focus on criminal pity, the *Cyber Security and Data Protection Bill* makes it clear that privacy does not extend to the state's surveillance apparatus. Ncube (2016, p. 99) is quite frank in describing the state of data privacy in Zimbabwe:

> [The] perceived and experienced vulnerability [of people's personal data] is exacerbated by the fact that there is a general lack of knowledge about existing legal protection of privacy. The legislative framework does little to assuage this vulnerability because it is currently inadequate.

Makulilo (2016, p. 372), considering the data privacy regimes in a number of African countries comparatively, states, "Zimbabwe [is] characterised

[among the] authoritarian states. The surveillance context in each of the countries in Africa partly reflects its democratic status."

Data protection and data colonialism

Finally, ARM professionals should maintain an awareness that data has become a resource, specifically, a resource that Western technological firms are trying to extract and exploit. Data protection laws are often posited as a solution to this problem but are even more inadequate to protect Africans' data privacy than they are to protect Americans' data privacy. According to Coleman (2019, p. 423), "[u]nder digital colonialism, foreign powers, led by the United States, are planting infrastructure in the Global South engineered for [their] own needs, enabling economic and cultur[al] domination while imposing privatized forms of governance." In other words, because there is so much economic value to be extracted by establishing a virtual monopoly in order to take Africans' personal data for advertising and predictive analytics, American companies like Facebook and Alphabet (the parent company of Google) are strongly incentivized to build (subpar) infrastructure – "poor internet for poor people" – in order to deliver those peoples' data to the companies (Biddle, 2017). While such companies have been vacuuming up Westerners' personal data for years now, the situations are not the same. In countries such as the United State, extensive Internet infrastructure is already in place, which allows greater access without being held captive by an entity such as Facebook.

Furthermore, "big tech companies can violate (and have blatantly violated) [data protection] laws, since they have the time, money, and resources to fight for their desired outcomes, even if they stand in direct violation of pre-established law" (Coleman, 2019, p. 433). Indeed, penalties and fines are simply a cost of doing business, and are far lower than the value that Facebook or Alphabet extracts from its illegal conduct. Even if the law could provide for consequences that would have a deterrent impact – as, arguably, Kenya's Data Protection Law could by – there is not guarantee of meaningful impacts. As Coleman argued prior to the Data Protection Law's passage: "[l]arge tech companies and data brokers could simply dissolve before they ever have to face any accountability measures" (Coleman, 2019, p. 435).

ARM professionals, then, are in the delicate position of having to ensure their compliance with data protection regulations while ensuring the trustworthiness of their records, and doing so in a way that takes advantage of all available resources without imposing undue risk. This challenge is amplified by data protection bills that are anything but, and digital colonists offering cheap "solutions" that impose new kinds of privacy problems.

Conclusion

ARM professionals must balance a number of competing requirements, values, and priorities, often in under-resourced environments, and in the face of sometimes incredible legal complexity. In Botswana, Kenya, South Africa, and Zimbabwe, they must balance the recordkeeping requirements of archives-specific laws with the transparency-needs from ATI-laws and the protection of data subjects' privacy and data. Furthermore, the letter of the law may well depart from the reality on the ground, like when an "access to information" law is used to limit the media and control dissent. Finally, ARM professionals in the countries in this study, operating as they do in post-colonial societies that are still navigating the fallout of colonization on both their legal and bureaucratic systems, must remain continuously aware of the power dynamics inherent in recordkeeping, and the values they and their institutions serve, and should serve. These professionals carry the heavy burden of meeting the requirements of the law while serving the needs of their whole community, including those whose voices are silenced, towards a better future. As Bhebhe and Ngoepe (2021, p. 155) remind us, "those who are oppressed would always find a way of expressing themselves and try to shape the world they want to live." ARM professionals must listen carefully for those expressions.

Notes

1 A table of laws and references examined is available on the InterPARES Trust website.
2 This is not, however, a universal view: "Eduard Fagan . . . says that there has been much support, both judicial and academic, for the view that South African law is a legal system in its own right" (Fombad, 2010, p. 6).

References

Abuya, E. (2013). 'Realizing the right of access to information in Kenya: What should stakeholders be on the lookout for?' in F. Diallo and R. Calland (eds.). *Access to information in Africa: Law, culture and practice*. Lieden: Brill, pp. 215–244.

Adeleke, F. (2013). 'Constitutional domestication of the right of access to information in Africa: Retrospect and prospects,' in F. Diallo and R. Calland (eds.). *Access to information in Africa: Law, culture and practice*. Leiden, Netherlands: Brill, pp. 83–105.

African Commission on Human and Peoples' Rights. (2002). *Declaration of principles on freedom of expression in Africa*. Available at: www.right2info.org/resources/publications/instruments-and-standards/africa_declaration-of-principles-on-freedom-of-expression-in-africa (Accessed 8 August 2021).

African Commission on Human and People's Rights. (2013). *Model law on access to information for Africa*. Available at: www.achpr.org/files/news/2013/04/d84/model_law.pdf (Accessed 7 December 2017).

African Commission on Human and Peoples' Rights. (2019). *Declaration of principles on freedom of expression and access to information in Africa*. Available at: www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf (Accessed 8 August 2021).

African Union. (2007). *African charter on democracy, elections and good governance*. Available at: www.right2info.org/resources/publications/instruments-and-standards/africa_charter-on-dem-elections-and-gov_2007_eng (Accessed 8 August 20210.

Balule, T. B. and B. J. Dambe. (2018). 'The right of access to state-held information in Botswana: Lessons from emerging international human rights jurisprudence,' *Commonwealth Law Bulletin*, 44 (3), pp. 429–451.

Bhebhe, S. and Ngoepe, M. (2021). 'Elitism in critical emancipatory paradigm: National archival oral history collection in Zimbabwe and South Africa,' *Archival Science*, 21, pp. 155–172.

Biddle, E. R. (2017). *The more we connect, the better it gets – for Facebook*. Available at: www.nytimes.com/2017/09/26/opinion/facebook-free-basics.html (Accessed 24 September 2021).

Botswana. (1978). *National archives and records services cap 59*. Available at: https://botswanalaws.com/alphabetical-list-of-statutes/national-archives-and-records-services (Accessed 20 July 2021).

Botswana. (2014a). *Electronic communications and transactions act 14 of 2014*. Available at: https://botswanalaws.com/alphabetical-list-of-statutes/electronic-communications-and-transactions (Accessed 20 July 2021).

Botswana. (2014b). *Electronic records (evidence) act 13 of 2014*. Available at: https://botswanalaws.com/alphabetical-list-of-statutes/electronic-records-evidence (Accessed 20 July 2021).

Calland, R. and Diallo, F. (2013). 'Introduction: Navigating the transparency landscape in Africa,' in F. Diallo and R. Calland (eds.). *Access to information in Africa: Law, culture and practice*. Lieden: Brill, pp. 1–9.

Chaterera, F. (2016). 'Managing public records in Zimbabwe: The road to good governance, accountability, transparency and effective service delivery,' *Journal of the South African Society of Archivists*, 49, pp. 116–136.

Chesworth, J. A. (2010). 'Islamic courts in Kenya and Tanzania: Reactions and responses,' The Centre for Muslim-Christian Studies Newsletter. Available at: www.cmcsoxford.org.uk/s/Chesworth-Islamic-Courts-in-Kenya-and-Tanzania-CMCS-News-10-02.pdf (Accessed 9 October 2021).

Clegg, M., Ellena, K. et al. (2016). *The hierarchy of laws understanding and implementing the legal frameworks that govern elections*. Arlington, VA: International Foundation for Electoral Systems.

Coleman, D. (2019). 'Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws,' *Michigan Journal of Race and Law*, 24 (2), pp. 417–439.

Cornell Law School. (2020). *Legal systems*. Available at: www.law.cornell.edu/wex/legal_systems (Accessed 23 September 2021).

Daigle, B. (2021). 'Data protection laws in Africa: A pan-African survey and noted trends,' *Journal of International Commerce and Economics*, pp. 1–27.

Darch, C. (2013). 'The problem of access to information in african jurisdictions: Constitutionalism, citizenship, and human rights discourse,' in F. Diallo and R. Calland (eds.). *Access to information in Africa: Law, culture and practice*. Leiden, Netherlands: Brill, pp. 27–53.

Da Veiga, A. (2020). 'Concern for information privacy in South Africa: An empirical study using the OIPCI,' *Information and Cyber Security 19th International Conference,* Pretoria, South Africa, Springer.

Diala, A. C. and Kangwa, B. (2019). 'Rethinking the interface between customary law and constitutionalism in sub-Saharan Africa,' *De Jure Law Journal*, 52 (1), pp. 189–206.

Fombad, C. (2010). 'Mixed systems in Southern Africa: Divergences and convergences,' *Tulane European and Civil Law Forum*, 25 (1), pp. 1–22.

Garner, B. A. (1995). *A dictionary of modern legal usage*. New York: Oxford University Press.

Georgiadis, K. M. (2012). *The emerging jurisprudence on the right of access to information in Kenya*. Available at: https://ssrn.com/abstract=2257151 (Accessed 23 September 2021).

Hofman, D. (2020). *Between knowing and not knowing: Privacy, transparency and digital records*. University of British Columbia, Vancouver. PhD thesis.

Katuu, S. (2011). 'Freedom of information in Africa,' in *Strengthening governance in the electronic environment: Managing records as reliable evidence for ICT/e-government and freedom of information*. Available at: www.researchgate.net/publication/322301296_Freedom_of_Information_in_Africa (Accessed 24 September 2021).

Katuu, S. (2020). 'Exploring the challenges facing archives and records professionals in Africa: Historical influences, current developments and opportunities,' in R. Edmondson, L. Jordan and A. C. Prodan (eds.). *The UNESCO memory of the world programme: Key aspects and recent developments*. Cham, Switzerland: Springer Nature, pp. 275–292.

Katuu, S. and Ngoepe, M. (2015). 'Managing digital records within South Africa's legislative and regulatory framework,' *3rd International Conference on Cloud Security and Management ICCSM-2015*. B. E. Popovsky. Tacoma, WA, USA, University of Washington – Tacoma, pp. 59–70.

Kenya Judiciary. (2021). *Structure of courts*. Available at: www.judiciary.go.ke/courts/ (Accessed 23 September 2021).

Khan, N. (2020). 'Custom, culture and law in colonial, anti-colonial and postcolonial times,' *Birkbeck Law Review*, 7 (1), pp. 1–25.

Khumalo, N. B., Mosweu, O., et al. (2016). 'A comparative study of freedom of information legislation in Botswana, South Africa and Zimbabwe,' *Mousaion*, 34 (4), pp. 108–131.

Lemieux, V. L. and Trapnell, S. E. (2016). *Public access to information for development: A guide to the effective implementation of right to information laws*. Washington DC: World Bank Publications.

Magina, A. (2019). *Access to information in Kenya: A critical analysis of the access to information act 2016*. University of Nairobi, Nairobi. Master's thesis.

Makulilo, A. B. (2016). 'The future of data protection in Africa,' in A. B. Makulilo (ed.). *African data privacy laws*. Cham: Springer, 33, pp. 371–379.

Malila, I. S. (2010). 'Reconciling plural legal systems: Between justice and social disorder in Botswana,' *Botswana Notes and Records*, 42, pp. 71–78.

Manganga, K. (2012). 'The internet as public sphere: A Zimbabwean case study (1999–2008),' *Africa Development*, 37 (1), pp. 103–118.

McLeod, J. (2019). 'The cloud: Challenges and issues,' in L. Duranti and C. Rogers (eds.). *Trusting records in the cloud: The creation, management, and preservation of trustworthy digital content*. London, UK: Facet Publishing, pp. 13–36.

Mosweu, T. and Simon, I. (2018). 'The implications of the national archives and records services act on archival practice in Botswana,' *Journal of the South African Society of Archivists*, 51, pp. 70–96.

Moyo, S. (2013). 'Regime survival strategies in Zimbabwe in the 21st century,' *African Journal of Political Science and International Relations*, 7 (2), pp. 67–78.

Mutsagondo, S. and F. Chaterera. (2016). 'Mirroring the National Archives of Zimbabwe Act in the context of electronic records lessons for ESARBICA member states,' *Information Development*, 32 (3), pp. 254–259.

Ncube, C. B. (2016). *Data protection in Zimbabwe*. *African Data Privacy Laws*. A. B. Makulilo. Cham: Springer, 33, pp. 99–116.

Ngoepe, M. and Saurombe, A. (2016). 'Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African Development Community,' *Archives and Manuscripts*, 44 (1), pp. 24–41.

Organisation of African Unity. (1981). *African charter on human and peoples' rights*. Available at: https://au.int/sites/default/files/treaties/36390-treaty-0011_african_charter_on_human_and_peoples_rights_e.pdf (Accessed 20 July 2021).

Osiro, R. (2013). 'Women's views on the role of Kadhi's courts: A case study of Kendu Bay, Kenya,' in J. Chesworth and F. Kogelmann (eds.). *Sharīʿa in Africa today: Reactions and responses*. Leiden: Brill, pp. 149–176.

Palmer, V. V. (2012). 'Mixed legal systems,' in M. Bussani and U. Mattei (eds.). *The Cambridge companion to comparative law*. Cambridge: Cambridge University Press, pp. 368–383.

Republic of Kenya (2010). *Kenya constitution*. Available at: www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010 (Accessed 21 July 2021

Right2Info. (2021). *Constitutional provisions, laws and regulations*. Available at: www.right2info.org/laws/constitutional-provisions-laws-and-regulations (Accessed 8 August 2021).

Shepherd, E., Stevenson, A., et al. (2011). 'Records management in English local government: The effect of freedom of information,' *Records Management Journal*, 21 (2), pp. 122–134.

South Africa. (1996). *National archives act 43 of 1996*. Available at: www.info.gov.za/gazette/acts/1996/a43-96.htm (Accessed 20 July 2021).

Van der Bank, C. M. (2012). 'The right to privacy – South African and comparative perspectives,' *European Journal of Business and Social Sciences*, 1 (6), pp. 77–86.

Van der Merwe, C. (2012). 'The origin and characteristics of the mixed legal systems of South Africa and Scotland and their importance in globalisation,' *Fundamina: A Journal of Legal History,* 18 (1), pp. 91–114.

Wallis, M. (2019). 'Interpretation before and after *Natal Joint Municipal Pension Fund v Endument Municipality* 2012 (4) SA 593 (SCA),' *Potchefstroomse Elektroniese Regsblad/Potchefstroom Electronic Law Journal*, 22 (1), pp. 1–29.

Wario, H. A. (2013). 'Debates on Kadhi's courts and Christian-Muslim relations in Isiolo Town: Thematic issues and emergent trends,' in J. Chesworth and F. Kogelmann (eds.). *Sharīʿa in Africa today: Reactions and responses*. Leiden: Brill, pp. 149–176.