Balancing and reconciling the conflicting values of information access and personal data laws in South Africa

Mpho Ngoepe

Department of Information Science,
Faculty of Human Sciences, University of South Africa,
Pretoria, South Africa

■ Abstract

Information access and protection of privacy (IAPP) laws sound like a contradiction in terms. However, both are internationally and constitutionally recognised rights as neither is accorded greater importance than the other. This raises a number of questions: ‘Does the right of access supersede the right to forget?’; ‘Does the privacy of a person override access to information?’; and ‘What if private information is in the public domain?’ There are many more questions than answers that require the balancing and reconciliation of these conflicting values of IAPP. This chapter proposes mechanisms for

How to cite: Ngoepe, M., 2021, ‘Balancing and reconciling the conflicting values of information access and personal data laws in South Africa’, in D.N. Ocholla, N.D. Evans & J. Britz (eds.), *Information knowledge and technology for development in Africa*, pp. 71–84, AOSIS, Cape Town. <https://doi.org/10.4102/aosis.2021.BK262.05>

balancing and reconciling IAPP with reference to laws in South Africa. The chapter analysed the IAPP laws in South Africa, that is, *the Promotion of Access to Information Act* (Act No. 2 of 2000) and *the Protection of Personal Information Act* (Act No of 2013) to identify the conflicting and complementary values. Literature was also reviewed on issues relating to IAPP. The chapter established the fact that although access to information has long been implemented in South Africa, IAPP laws have not yet fully grown. The privacy law was passed in 2013 but came into effect only on 01 July 2020. While the chapter acknowledges that both pieces of legislation embrace the writ 'habeas data', there is no outright answer to the challenge for balancing the two laws. However, some of the issues can be balanced through compatible definitions. Furthermore, there is complementary provision in the two laws as South Africa's right of access to information does make provision for refusal of information on the grounds of privacy. Furthermore, both laws make provision for access of one's own personal information held by public or private entities. The chapter provides ways in which implementing agencies and oversight mechanisms can balance the two rights to mitigate conflicting values. For example, the simple steps for organisations would be to identify relevant laws, identify records to which laws apply and ensure that records are created and handled in accordance with applicable laws. The study encourages proactive disclosure by implementing agencies to allow citizens to participate in decision-making in the public sector. This way the country will be considered advanced as citizens will be accessing information without lodging requests.

■ Introduction

Governments around the globe, including that of South Africa, have enacted freedom of information laws that allow access to organisations' records. In countries such as South Africa, this law is applicable to both private and public bodies. These laws include limited exceptions to withhold information contained in records and sometimes entire records from disclosure (Kozak 2015). A contradictory major legal consideration that governs access to information is the protection of privacy legislation. The intent of privacy legislation is to protect the privacy of individuals through the way in which data about those individuals are collected, used, managed, secured, stored, shared or destroyed. As Surtees (2010) would attest, public and private organisations that collect and use personal information have a responsibility to ensure privacy to the data subject. Privacy in this sense has to do with control over access to one's personal information (Pearce-Moses 2019). This, according to Surtees (2010), calls for the understanding of privacy issues that may arise from access to personal information and how to deal with the issues. Privacy in this regard relates to the right of a person and the relationship to society (Ngoepe, Mokoena & Ngulube 2010).

For a democratic society to thrive, the pieces of legislation governing the rights of IAPP need to be enacted. While the two laws sound like a contradiction in terms, both are internationally and constitutionally recognised rights as neither is accorded a greater right than the other. The two rights are taken seriously at an international level, for example, through 'Article 19 of the Universal Declaration of Human Rights' (UNDHR) and 'the International Covenant on Civil and Political Rights' (Mojapelo 2017). Furthermore, the rights are also implemented in most of the modern national constitutions as part of human rights. For Arko-Cobbah and Olivier (2016), the two rights, although conflicting, are a basis for other human rights. Despite the availability of laws worldwide for provisions allowing access in the form of records, there are still inconsistencies in privacy laws that make access difficult (Kozak 2015). However, the intention of passing privacy legislation was not to make access difficult. Examples of such laws include the European 'General Data Protection Regulation (GDPR)', Brazil's General Personal Data Protection Law, *Ireland's Data Protection Act*, the Canadian '*Personal Information Protection and Electronic Documents Act*' and South Africa's *Protection of Personal Information (POPI) Act* (Ngwenya 2020). These laws give people control over how businesses collect and process their information, although some commentators see it as an inhibiting factor for access to information. Other inhibiting factors to access to information, according to Ngulube (2006), include physical and intellectual control of information. In other words, put simply by Engvall (2019), access is limited if information cannot be retrieved when requested. As a result, as observed by Gafuik (2010), private citizens do not use the law to engage with government and hold governments accountable.

Whitman, McLeod and Hare (2001) posited that IAPP laws have brought about several challenges for many countries. The challenges include overlapping of rights, which could result in different solutions and conflicts, as well as decisions on requests. However, it should be noted that both rights are intended to help individuals to make public bodies and, in some instances, private organisations work transparently and accountably. Ngoepe et al. (2010) viewed the IAPP rights as complementing each other in holding public bodies accountable to taxpayers. Indeed, IAPP laws are focused on ensuring accountability, transparency and good governance by public bodies.

This chapter proposes mechanisms for balancing and reconciling IAPP laws in South Africa. Previous studies focused mainly on reviewing access to information since the legislation was enacted in 2000, as the *POPI Act* was only ratified in 2013 and came into effect on 01 July 2020. As a result, studies in South Africa have not been looking at the contradicting value of the two rights in legislation, as well as how the conflicting values can be balanced and reconciled. However, there have been studies conducted elsewhere such as those by Whitman et al. (2001), a working paper by Banisar (2011) for the World Bank, as well as a presentation by Beamish (2017), to mention just a

few, about 'protecting and balancing access and privacy rights'. Furthermore, in 2018, the student chapter of the Association of Canadian Archivists at the University of British Columbia presented its tenth annual international seminar and symposium on the issue of balancing access and privacy. In South Africa, a study by Kirkwood (2002) looked at the relationship between freedom of information legislation and archival law, while a study by Makhura and Ngoepe (2006) assessed compliance with both pieces of legislation by public bodies.

In this chapter, the background to IAPP will be provided first, followed by a discussion of IAPP legislation in South Africa, models of IAPP implementation, conflicting rights and how these can be balanced and reconciled. These laws are complex and adopted for a variety of reasons. The problem that is solved is that the two pieces of legislation can either complement or contradict one another, depending on the issue at hand. For example, in some instances, privacy laws can be used by public institutions when requesters demand access to records, which also include certain personal data. It happened in South Africa during the Zondo Commission on state capture when the records of the State Security Agency had to be used as evidence in the enquiry. There were opposing arguments on whether such records should be presented at the Commission. Therefore, this raises many questions: 'Does the right of access give way to the right to forget?', 'Does the privacy of a person override access to information?' and 'What if private information is in the public domain?' There are more questions than answers that require the balancing and reconciliation of these conflicting values of IAPP. There is a greater need for access to information for several reasons by individuals and civil society, including those with personal information. Requesters of information such as journalists, individuals and civil society would like to know why public bodies took certain decisions, while on the contrary, historians and academics seek information for research purposes (Banisar 2011).

■ Background to information access and protection of privacy

The issue of IAPP has been there and practised unconsciously since time immemorial. In ancient times, access to information was limited to the aristocracy and clergy as it was the exclusive purview of sovereigns or rulers (Onyancha & Ngoepe 2011). It was only during the enlightenment period (1685-1815) that access to records was extended to historical scholars. The idea of access to information was first conceived over 250 years ago in Sweden and today is recognised as the backbone of democracies. According to Ackerman and Sandoval-Ballesteros (2006), Sweden set the trend by passing the first Freedom of Information (FOI)URL legislation in 1766 which was titled the 'Freedom-of-Press and the Right-of-Access to Public Records Act'. This Swedish law allowed access to information to the public. It was only after the

French Revolution (1789–1799) that countries started to adopt archival and IAPP laws (Onyancha & Ngoepe 2011).

As indicated earlier, the concept of IAPP is catered for in many human rights instruments internationally by the UN, regionally and nationally (Nkwe 2020). In the African continent, Article 9(1) and (2) of ‘the African Charter on Human and People’s Rights’ makes provision for an individual to have the right to receive and disseminate information. Furthermore, in 2004, the African Charter on Human and People’s Rights adopted a resolution and created the position of the ‘Special Rapporteur on Freedom of Expression and Access to Information in Africa’ (Mojapelo 2017). Article 4 of SADC protocols against corruption compels the signatories to create a mechanism that promotes IAPP. In this regard, the SADC identifies access to information as one of the mechanisms that its member states can use to dismantle the acts of corruption.

Nationally, as already alluded to, many countries have adopted access to information legislation, for example, Australia, Canada, New Zealand and the United States, to mention just a few (Nkwe & Ngoepe 2021). In the 20th century, some European countries and the United States introduced freedom of information laws with the focus on access to records (Nkwe & Ngoepe 2021). For example, Lemieux and Trapnell (2016) indicated the adoption by ‘Finland (1951), United States (1966), Denmark and Norway (1970), France and the Netherlands (1978), Australia and New Zealand (1982), Canada (1983) and Colombia (1985)’, to mention just a few. This was followed by Eastern European countries such as Hungary, which implemented more rigorous versions of this legislation by reducing the period of compliance (Lemieux & Trapnell 2016). In Africa, South Africa took the lead by enacting the law in the year 2000. Adu (2018) argued that many African countries followed suit with 20 governments enacting such pieces of legislation. By 2018, over 100 laws throughout the world were ratified (Adu 2018). In Africa, some countries passed the legislation because of pressure from civil society. However, these laws are not without problems, as Adu (2018) identified a paradox in their implementation, such as lack of resources and government continuing to deny information.

In the digital era, the tide of access to information turned from openness amidst concerns of protection of personal information. The proliferation of technology has accentuated the growing need to collect and share personal information by the private sector. In this era, data on each of us are now constantly being collected and stored. This personal information is disseminated over networks such as social media platforms without the knowledge or consent of individuals. The government is perhaps the largest collector of data even though the private sector and, to some extent, individuals do collect personal data (Ngoepe et al. 2010). Billions of pieces of data exist on citizens. For example, when a person is born, enrolls at the college, applies

for social grants or driver's licence, gets married or even visits family members or friends in an estate residence, data are generated and stored somewhere in a computer database or mobile applications. A difficult question to answer, according to Ngoepe et al. (2010), is, 'Who owns this information?' Is it the government or individuals whose details are captured? If such data were collected by a public or private entity, does such an entity own the data and can such an entity use the data in any way it wants? In South Africa, for example, many people have experienced a situation where they receive anonymous calls from insurance companies selling them their (insurance companies') products. One wonders how and where these companies got hold of the contact details. A perfect, widely publicised example is when the late King Goodwill Zwelithini (1948–2021), the Zulu Monarch, fell victim to a pesky telephone call by a MiWay Insurance sales agent on 10 February 2018 to sell him the insurance product.⁶ If this can happen with such a high-profile individual, it could easily happen to anybody.

With today's technology, the right to privacy is becoming a challenge and therefore also hampers access to information. For example, mobile applications such as Glovisor, which is available on Android and other software, allow for the invitation of visitors and the creation of a PIN to allow access to the estate. The danger with this application is that, once the visitor arrives, the licence or identity document of such a person is scanned into the app. Both the host of the visitor and the estate will then have the personal information of the visitor. Such information needs to be protected by the estate as the collector, bearing in mind that a resident has access to the personal information of his visitors. Ngwenya and Ngoepe (2020) maintained that there are no measures in place to prevent the host from distributing such information.

This is compounded by what is termed 'post-truth'. Because of the increased use of the term 'post-truth', particularly during the presidential campaigns of Donald Trump in the 2016 election, as well as the European Union Referendum and the Brexit vote in the United Kingdom, it was named English 'Oxford Dictionary word of the year 2016' (Calcutt 2016). It is defined in the Oxford Dictionary as 'conditions in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief'. A similar phenomenon to post-truth is disinformation, that is, the deliberate propagation of information that is spread to confuse and by providing deceitful alternative versions of the facts. In other words, reliance on sources seems hopelessly mired in partisanship, while it becomes increasingly unclear who is responsible for the truthfulness of news stories, marketing and profiling. This is related to fake news as best stated by Pope Francis (2018) in his tweet that:

6. The call audio can be listened to here: <https://www.enca.com/south-africa/listen-zulu-king-scolds-blesses-miway-sales-agent>

The tragic history of human sin, is the first ‘fake news’ and it dates back to the book of Genesis, when the ‘crafty serpent’ lied to the woman. In present day, according to the Pope’s message the fast digital world helps fuel the spread of ‘fake news’ – which he defines as ‘the spreading of disinformation online or in the traditional media’. Disinformation thus thrives on the absence of healthy confrontation with other sources of information that could effectively challenge prejudices and generate constructive dialogue; instead, it risks turning people into unwilling accomplices in spreading biased and baseless ideas. (n.p.)

Information professionals such as archivists and librarians can play a role in raising awareness of the public by helping them to recognise misinformation by supporting the development of metaliteracy that helps people move beyond information literacy and digital literacy to understand how to interpret, evaluate and assess sources of information. The role can also be extended to the authentication of records. However, the technical infrastructures that gather and store data have become increasingly complex, often invisible and hidden. As a result, in the public space, archivists are at a loss to capture much, if any, provenance data about the information found there and, oftentimes, even to understand the scope and scale of these infrastructures and who controls them, which systems are overtly or covertly collecting their data or how to prevent them. For Duranti (2017), one of the means of authenticating such information is to use traditional archival principles such as diplomatics or digital records forensics. Mutula (2006) has rightly observed that governments often abuse privacy legislation to deny the public or individual access to information.

■ Information access and protection of privacy in South Africa

In South Africa, IAPP laws are provided for in the constitution, which was signed by the first president of democratic South Africa, Nelson Mandela (1994–1999) on 10 December 1996. This provision is stated in Chapter Two of the Constitution that contains the Bill of Rights listing a number (27) of rights. Among the listed rights is access to information that gives citizens ‘access to any information held by the state for the protection of his or her rights, as well as the right to privacy’, which is one of the fundamental rights. For example, Section 14 of the Constitution is about the right of privacy to everyone. Both privacy and access maintain that privacy is a valued right.

In South Africa, IAPP laws consist of the *Promotions of Access to Information Act* (PAIA) and *POPI Act*. The oversight mechanism for PAIA since enactment in 2000 has been the South African Human Rights Commission (SAHRC) until 2015, when the Information Regulator was established in terms of the *POPI Act* (Mojapelo & Ngoepe 2017). Around 2016, when the office of the Information Regulator became operational, the regulatory role of the IAPP laws was moved to this office from the SAHRC (Mojapelo 2017).

On the contrary, the *POPI Act* was passed in 2013 but came into effect only in 2020. The enforcement of the law was delayed to allow the establishment of the regulatory bodies (Ngwenya 2020). The passing of the law was done to align South Africa with international data protection best practices such as GDPR (Ngwenya 2020). The *POPI Act* was passed to promote the constitutional right to privacy by protecting personal information. In this regard, as observed by Ngwenya and Ngoepe (2020), POPI guarantees that all organisations in:

South Africa behave responsibly when collecting, processing, storing, and sharing personal information by holding them accountable, should they abuse or compromise that entity's personal information in any way. (p. 8)

According to De Bruyn (2014), the *POPI Act* regulates:

[T]he manner in which personal information may be processed by established principles, and provides persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act. (p. 1316)

The following summarises the aim of the Act:

- When and how a person decides to share his or her data (requires individual permission).
- The degree to which a person elects to share data.
- Transparency, responsibility and accountability regarding how the person's information will be utilised (restricted to the purpose) and warning if or when the information is used for the wrong reasons.
- Providing the person access to their data and the right to have it deleted should the data subject wish to do so.
- Who can access the personal data?
- Storage of personal data (measures and controls have to be in place to shield private data).
- The authenticity of personal data (e.g. personal data must be captured correctly once collected and the institution must look after the personal information in a responsible manner).

Of interest are the provisions of the *National Archives and Records Services of South Africa Act* (NARSSA) (Act No. 43 of 1996) and PAIA regarding access to records contained in archives and public records. This Act provides unrestricted access to archives in the custody of archives repositories after 20 years, calculated from the end of the year in which a particular document was created. According to Kirkwood (2002), as the open period is extended annually, the closed period should never be longer than 21 years as per Section 12(1)(a) of NARSSA. The only ground for refusing access relates to the fragile condition of a record, and there is a right to appeal to the National Archives Advisory Council. It should be noted that the provisions of PAIA take precedence over NARSSA with regard to access to information contained in records, both in the closed and open periods and whether or not they are in archival custody.

■ Models of information access and protection of privacy implementation

There are different models of implementing IAPP laws in different countries in order to ensure synergy. In many countries, especially in the Caribbean, the IAPP laws are linked in the constitution through the concept of '*habeas data*', that is, 'a right that allows people to request access to their own information and to control its use can both complement and conflict with each other'. The models identified include single access to information and privacy law. For example, the Canadian law implemented in 1982, as well as the Hungarian law and Zimbabwean law. It is worth noting that with effect from 1 July 2020, the Zimbabwean government signed into law *the Freedom of Information Act* (No 1 of 2020), repealing the access to information and privacy law and thus dividing it into two. The Canadian IAPP legislation has been enacted as one Act. This model makes provision for shared definitions, ensures consistency, limits conflict and establishes balance from the start. Furthermore, in Canada, individual provinces have passed their IAPP legislation; for example, British Columbia province has its own legislation in the form of *Freedom of Information and Protection of Privacy Act* (Nkwe & Ngoepe 2021). The other model can be one law and few provisions for the other. Until 2017, in South Africa, the IAPP laws were disjointed and regulated by different regulatory bodies (Nkwe 2020). In this regard, PAIA was regulated by SAHRC, while the *POPI Act* was regulated by the Ministry of Intelligence (Mojapelo 2017; Nkwe 2020). PAIA has a concomitant imperative to protect legitimate needs for confidentiality and secrecy.

The third model separates access to information and privacy law. South Africa is currently using this model with two pieces of different legislation, which are PAIA and the *POPI Act*. To ensure harmony in this regard, the two laws use common definitions, there are privacy exemptions in access to information law, provision is made in both laws for subjects to access personal information and there is provision for an oversight mechanism from one regulator and appeal process. This is also the case in the United Kingdom, where access to information legislation (Shepherd, Stevenson & Flinn 2009):

[P]rovides for the Information Commissioner to oversee the freedom of information (and the Data Protection Act), as well as acting as adjudicator if a request for access to information has been declined. (p. 229)

A key factor here is to balance both rights, and hence, perhaps Shepherd and Ennion (2007:34) argued that 'it explains the dual role of the Information Commissioner'. Furthermore, Shepherd and Ennion (2007) are of the view that although:

[F]reedom of information in the United Kingdom was intended to make the machinery of government more accountable and transparent, many of the exemptions provisions put in place seem restrictive and fail to protect the privacy of individuals. (p. 34)

On the contrary, in the United States, privacy laws are spread across many laws and enforcement agencies, for example, medical records.

■ Conflicts of access to information and personal privacy rights

Because of their conflicting nature, privacy and right to information are often regarded as the head and tail of a coin. However, Surtees (2010) is of the view that privacy law should not just be seen as the 'B' side of access to information but instead as existing in a somewhat symbiotic relationship. As already discussed, PAIA, along with the *POPI Act*, has created new challenges for those responsible for implementing IAPP laws. The essence of PAIA is to simplify the provision of access to information in government and private bodies. Although the IAPP laws have been enacted to accommodate information access and privacy, and although they are supposed to complement one another, by their nature, there is a potential tension for them. The essence of the *POPI Act* is to protect the individual's privacy right. Resolving the conflict between information access and privacy is a daunting task.

One of the conflicts may arise from a lack of understanding of what needs to be protected. As observed by Nkwe and Ngoepe (2021), some:

[R]ecords held by public entities contain information that identifies officials who were involved in the subject at some point such as the names of officials who wrote reports, attended meetings and endorsed decisions. (p. 3)

For example, in 2008, I was part of an interview panel for a candidate who was to report to me. The candidate who was appointed to the position was not the one I recommended. When the person resumed duty, as the records manager, she had access to the documentation of the selection process. She wanted to know why I did not recommend her, and this affected our working relationship. This can also happen with a student file. As much as universities claim that the examination for theses and dissertations is anonymous, if the student or supervisor requests access to the file, they will be able to establish who the examiners were. This is compounded by the lack of global consensus about the definition of personal information. However, in some instances, commentators argue that if it is done in an official capacity, it is not considered personal, as long as information regarding the life of an individual is not divulged. For elected officials, it is less restricted and personal information might even be divulged with the argument that public interests override all grounds for refusal of access to information. According to Donaldson and Lohr (1994), many governments took the position to not consider 'information relating to official capacities a personal information'. Although the information may be regarded as personal as it is about 'a particular identifiable person, generally, it is not related to his or her personal or family life and is less likely to be sensitive' (Donaldson & Lohr 1994). There is also consensus that

'information about elected or high-ranked public officials should be less restricted, even when it relates to their personal lives' (Donaldson & Lohr 1994). An example can be that of a confidential medical record of the late Minister of Health in South Africa, Dr Manto Tshabalala-Msimang (1999–2009), which was in the possession of the *Sunday Times* newspaper in 2007. Her lawyers used Section 17 of the *National Health Act* (Act No. 61 of 2003) to compel the *Sunday Times* to return the file. This may be because the *POPI Act* had not yet been enacted when the incident happened. According to Ngoepe et al. (2010), privacy should not be used as an obstacle for access to information where there is public interest. What needs to be a consideration is the extent to which access to a person's private information can be gained. Clearly, the right to privacy is not an absolute right, nor is it a comprehensive value. A person's right to claim privacy cannot be used as a defence to cover up or condone illicit acts. Both rights of access to information and privacy are important and relevant in a democratic society to contribute towards accountability, transparency and good governance.

A further conflict arises when government or institutions misuse privacy exemption or law to deny access to information. This was an issue in a case between the South African History Archives (SAHA) having to wait for six years to win a court battle against 'the central bank in South Africa to access records of foreign exchange fraud, Eskom bonds and gold smuggling during the apartheid years' (Independent Online Newspaper 2020). This came after the Supreme Court of Appeal found the decision of the South African Reserve Bank (SARB) to refuse access to the records of the late 'Brigadier Blaauw, Robert Hill and Vito Palazzolo in terms of PAIA application unlawful and in conflict with the provisions of the Act' (Independent Online Newspaper 2020). In the request by the SAHA, the SARB failed to respond within the prescribed time (30 days in terms of PAIA), but later refused access to records indicating that it was unable to retrieve records relating to the requests. In this regard, the refusal was because of a lack of physical and intellectual control of records, as well as a claim by the SARB that the records constituted personal information. In South Africa, the weaknesses in IAPP implementation have always been identified as the length of time being taken to process requests, that is, 30 days; access and request fees, which amount to R15 and R35, respectively, as well as ineffective means for resolving disputes under the Act, for example, the case of the SAHA having to pay about R5000 to access records of the Truth and Reconciliation Commission (TRC) in the custody of the NARSSA. The SAHA has tested the parameters of PAIA through a request of access to military records, nuclear records, TRC records and gay and lesbian records. In the process, the organisation also built up an archive of material released to the public in terms of PAIA. In this regard, the SAHA has a collection of records released under PAIA as they are in a public domain. These materials are scanned and digitised. One pundit argued that these records are exempted from copyright laws as they are in the public domain. The provenance of the

records is ensured through cataloguing and cross-reference to the originals. However, this raises an ethical question about personal information in such collections, especially with regard to restrictions in terms of the *POPI Act*. Access to these records is available to researchers free of charge. Of interest are British Columbia's FOI and privacy laws that indicate that it is no longer a privacy invasion to disclose personal data about a person who has passed on for 20 years or more or if the record has been in existence for 100 years or more (Kozak 2015). This also exists in the *UK FOI Act*, which indicates 30 years as historical.

■ Balancing and reconciling the values

According to Beamish (2017), 'the right of access to information and privacy laws are not always conflicting rights as they are both designed to ensure accountability'. It is therefore important how the oversight mechanism and implementing agencies balance the two. Despite the fact that FOI laws allow for a legal mechanism to access records, they also include limited exceptions to withhold information contained in records, and sometimes even entire records, from disclosure. Even though access under the FOI is defined as a legal right, there are provisions where government organisations can, or must, withhold records or information (Kozak 2015), for example, frivolous or vexatious requests and published information; however, in instances like these, the entity should 'direct the requester to the published source'. The IAPP legislation is supposed to make provision 'for strict time limits for the processing and finalisation of requests' (Banisar 2011). Where a request is refused, such refusal should be accompanied by comprehensive written reasons. If access is not granted, the requester can appeal through an internal appeals mechanism, which is referred to as a relevant authority. In South Africa, in the case of national departments, the relevant authority is the minister; in provincial departments, it is the member of the executive council; and for municipalities, it is the mayor. As it appears in Article 19 of UNDHR, 'all individual requests for information from public organisations should be met unless the entity can show that the information falls within the scope of the limited regime of exceptions'. To justify the refusal to grant access, the public entity is required by Article 19 of UNDHR to meet a 'strict three-part test' as follows:

- The information must relate to a legitimate aim listed in the law.
- Disclosure must threaten to cause substantial harm to that aim.
- The harm to the aim must be greater than the public interest in having the information'.

Sections 33–45 of PAIA provide 'grounds for refusal of access to information', which is divided into two categories, the first of which is mandatory grounds where access must be refused. An example of mandatory grounds for refusal

is if the requested records can affect a third party or the security of an organisation, an individual or a country. In that regard, access must be refused. The second ground for refusal is discretionary grounds where access can be refused, but it must not be refused. In this regard, the information officer should use his or her own discretion. Unlike FOI laws, which apply predominantly to government organisations, jurisdictions that have adopted privacy laws have made these laws applicable to both governmental and non-governmental organisations. These laws tend to rely on an individual's consent and reasonable actions taken given particular circumstances governing how personal information should be managed and accessed. An example includes *Personal Information Protection and Electronic Documents Act* (PIPEDA) in Canada and POPIA in South Africa.

■ Conclusion

Although the two rights seem to be opposing each other in nature, they are not always conflicting rights as there are some elements of compatibility. For example, PAIA, which is a freedom of information legislation, does, however, make provision for mandatory and discretionary grounds to deny access on the basis of privacy. There is a complementary provision in the two laws. Complementarity is achieved through ensuring accountability by the government to citizens. For example, both IAPP laws provide a person with the right of access to own personal information held by any organisation, as well as how personal information is handled. Information access and privacy protection are both constitutionally recognised rights. Therefore, neither is accorded a greater right than the other, although privacy may have a constitutional human right with a stronger position than access to information access. However, freedom of information law can be utilised to enhance privacy. When a state has both IAPP laws as in the case of South Africa, the approach is to use the privacy legislation to 'requests for personal information while requests for information that contains personal data about other parties could then be handled through the freedom of information legislation' (Beamish 2017). However, PAIA also provides that, 'in the absence of other legislation, public and private bodies must make reasonable efforts to establish internal measures to correct personal information held by the relevant bodies'.

From the discussion, this chapter reveals that PAIA has enabled organisations such as the SAHA to build up a substantial archive of released materials and make it accessible to the public. The question that needs further interrogation is 'can we build a public archive based on records requested in terms of PAIA?' If yes, how will the issue of copyright be addressed. Further questions and issues that need to be discussed include:

- The right to be forgotten versus the right of access.
- Does the right to forget overrides the public interest?

- Privacy versus historical research.
- Does public interest override or trump all grounds for refusal?
- What if private information is in the public domain?
- Can we use access to information to promote privacy?
- Can we use privacy law to obtain information?

As it can be seen from the discussion, the balancing of the two rights can be mitigated through clear compatible definitions and guidelines. It is important how implementing agencies and oversight bodies balance the two rights. Three simple steps to ensure implementation and harmony are: identify relevant laws and regulations relating to privacy and access to information; identify records to which laws or regulations apply and ensure records are created and handled in accordance with applicable laws or regulations. Otherwise, as Darch and Underwood (2010) have observed, the IAPP 'as an idea and culture has not yet taken root in South Africa because of a number of factors' such as awareness by citizens and poor management of information by the public sector. IAPP can be considered fully-fledged in South Africa when citizens can access information without lodging a request through the legislation. One of the limitations of this study is that it was undertaken when the privacy law in South Africa was not yet operational. An empirical study to explore the readiness of organisations in implementing privacy legislation is recommended.