CURRENT DEVELOPMENTS

Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa

I Introduction

The South African Law Reform Commission has proposed legislation to regulate what is variously referred to in international jurisdictions as 'data protection' and 'information privacy protection'.[1] The Law Commission's own formulation of the basic subject-matter of its proposals is 'protection of personal information'.[2] It has accordingly short-titled its proposed legislation, the Protection of Personal Information Act. If this name sticks and the legislation is enacted, it will in all likelihood, given the South African fondness for clunky acronyms, become known as the POPIA. Personal information (a term of art meaning information, irrespective of the medium in which it appears, that reveals something about someone[3]) is, in the Commission's proposals, to be protected by a complex regime of rights and remedies aimed at regulating its collection and dissemination and the uses to which it may be put. Along the familiar lines of the European model for data-protection regimes, the Commission's proposed legislation centres on a set of 'information protection principles' which flesh out a general and higher-level requirement that personal information must be processed 'in a reasonable manner in order not to infringe the privacy of the data subject'.[4]

The 'European model' referred to above stems from a number of international instruments which, though principally intended to regulate the transborder flow

1 SA Law Reform Commission 'Privacy and Data Protection', Discussion Paper 109 (October 2005), <http://www.doj.gov.za/salrc/dpapers.htm>. The Discussion Paper followed an earlier Issue Paper on the same topic (SA Law Reform Commission *Privacy and Data Protection* (Issue Paper 24 August 2003). The Commission's project committee on privacy and data protection is currently considering a large volume of comments received on the Discussion Paper prior to finalising its recommendations, likely to be published by the end of 2007. These recommendations are made to the Minister of Justice who will make the decision whether to introduce the legislation in Parliament. On the Law Reform Commission's processes and working methods, see <http://www.doj.gov.za/salrc/docs_gen/function.htm>. For a comparative overview of the subject, see A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 *SALJ* 400.

2 See the long title and clause 1 of the draft Protection of Personal Information Bill in Annexure B of the Discussion Paper (ibid) ('draft Bill' or 'POPIA').

3 See the definition of 'personal information' in clause 1 of the draft Bill. The corresponding term in the European instruments is 'personal data', but the Law Reform Commission has opted to use the term 'personal information' as it is also employed in the Promotion of Access to Information Act 2 of 2000 ('PAIA').

4 Clause 7 of the draft Bill. 'Data subject' means, according to the definitions in clause 1, the person to whom personal information relates. While the data subject is the principal right-holder under the draft POPIA, the principal duty-bearer is termed the 'responsible party', defined as 'the public or private body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal information'. The corresponding term in the European instruments (see note 5 below) is 'controller'.

of personal data, have had a great deal of influence on domestic laws regulating data protection.[5] The extent of this influence has resulted in what Lee Bygrave terms 'regulatory convergence', a family resemblance in the data protection laws that have mushroomed around the world since the earliest attempts to deal with the threats to privacy posed by computerised storage of personal data in the 1970s. In most jurisdictions, data protection follows the same basic recipe. According to Bygrave 'most of the laws take the form of so-called "framework" laws: instead of stipulating in casuistic fashion detailed provisions for regulating the processing of personal information, they set down rather diffusely formulated general rules for such processing, and make specific allowance for the subsequent development of more detailed regulatory norms as the need arises.'[6] The responsibility for developing the detailed norms referred to is usually given to an independent regulator, typically called a 'data protection authority'.[7]

The Law Reform Commission's proposals follow this recipe assiduously. Application, amplification and enforcement of the information protection principles will, in the first instance, be the job of a regulatory authority to be called the Information Protection Regulator.[8]

Our focus in this note is twofold. We consider the adequacy of the proposed regulatory authority when measured against the international standards in this regard. Secondly, we consider the Law Reform Commission's further recommendation that its proposed Information Protection Regulator should also have jurisdiction over the Promotion of Access to Information Act.[9] This is an interesting proposal which ought to be supported. It restores, as we show, aspects of the original design for the Open Democracy Bill, a document which has been the basis of much of South Africa's post-transition transparency legislation. It also has the prospect of curing one of the clearest defects in the

5 The Council of Europe's 1981 Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (COE Convention) and the OECD's 1981 Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (OECD Guidelines). The OECD Guidelines, structured around a set of Principles for the lawful processing of personal information, have been extremely influential in the development of the information privacy laws of a number of domestic jurisdictions. This is true also of the SALRC draft legislation. Another crucial international development is the European Union's 1995 Data Protection Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Directive). See L Bygrave *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002) 30-6.

6 L Bygrave 'An International Data Protection Stocktake at 2000: Part 1: Regulatory Trends' (2000) 6 *Privacy Law & Policy Reporter* 129, 130.

7 Ibid. Every jurisdiction with data protection legislation has some form of data protection authority. The only notable exceptions are the United States and Japan.

8 Earlier versions of the Commission's draft legislation used the nomenclature 'Information Protection Commissioner' and 'Information Protection Commission'. See Chapters 5, 7 and 8 of the draft Protection of Personal Information Bill (note 2 above). In more recent drafts, this has been substituted with the term 'Regulator' in order to clarify the function of the institution: it is intended to be a regulatory authority with the principal function of enforcement of the rights and duties in the legislation rather than the promotion of the ideal of data protection.

9 See para 4.2.207 in Chapter 4 of the Discussion Paper (note 1 above). It is intended that, should this proposal be approved, the powers and duties of the Commission as currently provided for in the draft Bill will be extended and consequential amendments will be made to the PAIA.

current access to information regime — the absence of an independent, accessible and authoritative mechanism for the resolution of information access disputes, other than resort to the courts.

II Enforcement of the Promotion of Access to Information Act: A Brief History

(a) The Open Democracy Bill

Data protection has been on the South African legislative agenda since 1994. In that year, a Task Group on Open Democracy was appointed by Deputy-President Mbeki.[10] The Task Group had the brief of considering the legislative changes that would be needed to build what the interim Constitution called an 'open and democratic society'[11] on the unsuitable foundation of the authoritarian and secretive apartheid state. The Group produced a set of policy proposals in January 1995,[12] recommending that an Open Democracy Act was needed to give effect to the constitutional ideal of an open and democratic society and a transparent and accountable government. The Group's draft Open Democracy Bill[13] was presented to Cabinet in 1996.

The draft Open Democracy Bill proposed by the Task Group had four principal parts: (1) freedom of information legislation applicable to information held by government bodies (Part III of the draft Open Democracy Bill); (2) data privacy legislation providing for the correction of and protection against unauthorised use of personal information held by both government and private bodies (Part IV);[14] (3) open meetings legislation requiring government meetings to be open to the public (Part V); (4) legislation for the protection of whistleblowers (persons who disclosed evidence of a contravention of the law

10 The team was able to draw on comparative work by one of its members, Professor Etienne Mureinik, on a draft South African Freedom of Information Act, done for the Administrative Law Reform Project of the Centre for Applied Legal Studies (CALS) in 1993. See J White 'Open Democracy: Has the Window of Opportunity Closed?' 1998 (14) *SAJHR* 65, 65-7. On the work of the CALS project see further, L Johannessen & J Klaaren & J White 'A Motivation for Legislation on Access to Information' (1995) 112 *SALJ* 45.

11 See s 33 and s 35(1) of the Interim Constitution (Constitution of the Republic of South Africa, Act 200 of 1993).

12 Task Team on Open Democracy 'Open Democracy Act for South Africa: Policy Proposals' (1995).

13 The draft Bill is available at <http://www.polity.org.za/html/govdocs/bills/1995/odb9/toc.htm>.

14 This Part of the Bill was intended, according to the POLICY PROPOSALS, 'to protect privacy' (note 12 above, 2). (It should be noted that the Task Group's work preceded the enactment of the Constitution of the Republic of South Africa, 1996 which, compared to the interim Constitution, expanded the scope of the constitutional right of access to information to include private bodies.) Part IV was not a particularly good fit with the remainder of the Bill which was principally concerned with the aim of promoting governmental transparency. The privacy component of the Bill aimed at strengthening the rights of the individual in relation to personal information by providing an expedited procedure for obtaining access to information about the requester (ie, it was made easier to obtain your own information than other information); a right to seek the correction of personal information; regulation preventing the improper use of personal information. Unlike the access to information and government-in-the-sunshine parts of the Open Democracy Bill, this aspect of the legislation applied also to information held by private bodies.

or maladministration) from civil or criminal liability, or from employment-related disciplinary procedures (Part VI).

Substantial modifications were made to this draft by Cabinet[15] and by Parliament, principally at the committee stage of the Bill by the Ad Hoc Joint Committee on the Open Democracy Bill.[16] For current purposes, the most important of these modifications was the removal of the data-protection chapter of the draft Bill. Explaining this change, the Committee reported to Parliament its recommendation that the Bill (which had by now been renamed the Promotion of Access to Information Bill) should deal only with the issue of access to personal information and not with other privacy-related interests in relation to such information (such as its control and correction).[17] These interests, in the Committee's opinion, were better protected by purpose-specific privacy and data protection legislation, along the lines of data protection statutes in numerous other jurisdictions. The Minister was requested to consider the introduction of such legislation in Parliament. This request was then referred by the Minister to the Law Reform Commission and is the origin of the Commission's investigation into privacy and data protection legislation.[18]

(b) Proposals on the enforcement of the Open Democracy Bill[19]

An earlier casualty, this time of Cabinet's changes to the Open Democracy Bill, was the Task Group's proposals on the enforcement of the provisions of the Bill. The Task Group had envisaged that proper implementation of the Bill would require administrative measures intended to perform two distinct functions:

- a *promotional* function: an entity must be established or an existing entity should be given the tasks of publicising the rights created by the Open Democracy Bill, educating the public and officials about the Bill, assisting members of the public to make requests for access to information, conducting research and publishing explanatory material about the Bill, monitoring the Bill's implementation and the use that is made of it and reporting to Parliament.
- an *enforcement* function: for the rights created by the Open Democracy Bill to be enforceable there should be a dispute-resolution process by which disputes over access to records can be resolved by an independent entity with the power of making authoritative and binding decisions.[20]

15 After considering the draft Bill for more than a year, Cabinet introduced a modified version of the Open Democracy Bill into Parliament as Bill 67 of 1998.

16 The principal purpose of the Parliamentary amendments was to give more comprehensive effect to the right of access to information in private hands (s 32(1)(b) of the Constitution of the Republic of South Africa, 1996) than either the draft Bill or Bill 67 of 1998 had done. See, further, I Currie & J Klaaren *The Promotion of Access to Information Act Commentary* (2002) [1.9].

17 See the account of the Committee's report in paras 1.1.2—1.1.5 of the Discussion Paper (note 1 above).

18 Ibid 1.1.4– 1.1.5.

19 Some of the material in this and the following section is drawn from research commissioned by the South African Human Rights Commission. See South African History Archive 'Strengthening the Role of the South African Human Rights Commission in Relation to the Promotion of Access to Information Act' in SA Human Rights Commission *Report on the Proceedings of the PAIA Indaba* (January 2004) 131-61.

20 Policy Proposals (note 12 above) 8-13.

Having drawn this distinction, the recommendations of the Task Group in relation to enforcement were the following:

- *Information officers*: each government body should appoint an official to consider requests for access to information held by that body.
- *Internal appeals*: if a request for information is refused the requester should be entitled to appeal to the head of the public body.
- *Information Court*: if the internal appeal is unsuccessful the requester would be entitled to appeal to an Information Court. This was envisaged as a superior court, established in each division of the High Court and staffed by High Court judges but operating under rules designed to ensure that they were accessible, cheap, simple, informal and expeditious.[21]
- *High Court*: the decisions of the Information Court would be reviewable in the High Court on administrative-law grounds.

The recommendations of the Task Group on the *promotion* of the rights created by the Act were the following:

- *Public Protector*: the Public Protector[22] would have the responsibility of facilitating the exercise of the rights in the Act by, variously: intervening on behalf of an information requester; mediating between the requester and the government; investigating complaints about maladministration of the Act and making recommendations to the government or Parliament; representing requesters, or intervening in the public interest before an Information Court or the High Court.
- *South African Human Rights Commission*: the SAHRC[23] could intervene in cases when the rights created by the Act overlapped with the constitutional right of access to information. This could entail investigating any alleged violation of rights and assisting anyone adversely affected by the violation to secure redress.[24]
- *Open Democracy Commission*: a small, independent Commission should be established to monitor the effectiveness of the Act and to report annually to Parliament. The Commission could propose amendments to the Act based conclusions drawn from its monitoring of the implementation of the Act.

(c) Enforcement provisions of the Promotion of Access to Information Act

The cabinet opted not to accept the Task Group's recommendations on the establishment of Information Courts and an Open Democracy Commission. The Open Democracy Bill, in the form in which it was introduced in

21 Policy Proposals (ibid) 8-9. A specialised information tribunal was considered by the Task Group as an alternative to the Information Court but was ultimately rejected by it on the grounds of cost. See ibid, 8 note 2.

22 Established by ss 181-2 of the Constitution and the Public Protector Act 23 of 1994.

23 Established by s 181 and s 184 of the Constitution and the Human Rights Commission Act 54 of 1994.

24 Policy Proposals (note 12 above) 10.

Parliament,[25] provided instead for disputes over access to information requests (after exhaustion of an internal appeal process in the case of public bodies) to be litigated in the High Courts. The Bill was then substantially amended during the Parliamentary process.[26] In the Promotion of Access to Information Act as enacted, the dispute-resolution and promotional duties that had been identified by the Task Team were re-allocated as indicated in the following table:

Table 1: Allocation of dispute-resolution and promotional duties

Duty	Draft Open Democracy Bill[27]	Promotion of Access to Information Act
Promotional duties		
Statistical monitoring and annual report to Parliament	Open Democracy Commission	SAHRC[28]
Annual review of Act and other laws bearing on openness and recommendations for amendment	Open Democracy Commission	SAHRC[29]
Monitoring of implementation and administration of the Act	Open Democracy Commission	SAHRC[30]
Development and conducting of educational programmes for the public and for officials; promotion of the objects of the Act among bodies	Open Democracy Commission	SAHRC[31]
Publication and dissemination of a guide on the Act	Open Democracy Commission	SAHRC[32]
Receiving and archiving manuals	Open Democracy Commission	SAHRC
Assisting requesters to make requests	Public Protector	SAHRC[33]
Receiving and investigating complaints about maladministration of the Act[34]	Public Protector	Public Protector[35]

25 Bill 67 of 1998.

26 The drafting history of the Bill up to its enactment as the Promotion of Access to Information Act is recounted in Currie & Klaaren (note 16 above) [1.7]—[1.9].

27 The Bill proposed by the Task Group on Open Democracy and presented to Cabinet in 1996. See note 13 above.

28 Section 84 of the PAIA.

29 Ibid s 83(3)(a).

30 Ibid s 83(3)(b).

31 Ibid s 83(2).

32 Ibid ss 10 and 83(1)(a).

33 Ibid s 83(3)(c).

34 Though neither the draft Open Democracy Bill nor the PAIA is particularly clear about this, it seems that the intention was for the Public Protector to investigate maladministration in the sense of a failure by a body to comply either on a systemic or individual level with the duties imposed by the Act. It was not intended that the Public Protector investigate the merits of any substantive dispute about the interpretation or application of the Act (eg, the merits of a refusal to grant access on one of the grounds listed in the Act). This was the province of the appeal provisions and the Information Courts.

35 Section 91(b) of the PAIA.

Enforcement duties		
First-instance internal appeals against refusals of requests, against fee decisions, against slowness or non-responsiveness.	Internal appeals to heads of public bodies	Internal appeals to heads of type (a) public bodies. No internal appeals for type (b) public bodies or for private bodies.
Appeals to independent tribunals	Appeals to Information Courts Administrative-law review of Information Court decisions by High Court	Appeals to magistrates courts[36] or High Courts. No review of High Court decisions.[37] Appeals against magistrates' court decisions.

Table 1 indicates that in both versions of the legislation:

- There is a rigid separation of the functions of promotion and enforcement: the former is to be performed by the Open Democracy Commission (in the ODB) and the SAHRC (in the PAIA); the latter is to be performed by Information Courts (in the ODB) or by the High Court (in the PAIA). The model adopted by many foreign jurisdictions,[38] of having a specialised information commission with duties of promotion and powers of dispute-resolution was not followed.[39]
- A further distinction is made in the legislation between dispute-resolution in the sense of disputes over the substance of access decisions made in terms of the Act and dispute-resolutions about what can be called administrative failures or maladministration of the Act. The former type of dispute is the province of the courts. The latter type of dispute is the province of

36 In terms of the definition of 'court' in s 1 of the PAIA, the courts with jurisdiction to hear appeals under the Act are the Constitutional Court, High Courts and magistrates' courts 'designated by the Minister . . . and presided over by a magistrate . . . designated in terms of s 91A'. All magistrates' courts have been designated as courts in terms of s 1: GN 938 of 27 June 2003.

37 This appears to be the effect of the ouster in para (ii) of the definition of 'administrative action' in the Promotion of Administrative Justice Act 3 of 2000: 'any decision taken, or failure to take a decision, in terms of any provision of the Promotion of Access to Information Act, 2000' is not administrative action.

38 See, for example, Ireland. The Irish Freedom of Information Act 1997 creates an Information Commissioner with powers to review the decisions of public bodies and to make binding decisions on access to records. The Commission also has a number of tasks that could be categorised as promotional: reviewing the operation of the Act, fostering attitudes of openness in government bodies and encouraging voluntary disclosure of information and the publication of guidance material on the practical operation of the Act.

39 The reason, it seems, was financial. See the comments by Johnny de Lange MP, erstwhile Chair of the Ad Hoc Parliamentary Committee at the PAIA Indaba (*Proceedings* note 19 above, 12): 'The Committee was in favour of an information commissioner, like in Australia and other countries . . . the Minister . . . did not want to commit to it, because clearly there are enormous financial implications'.

the Public Protector. The Public Protector is therefore given a role similar to that performed by the Ombudsman in jurisdictions such as Australia.[40]

(d) Evaluating the performance of the enforcement institutions under the PAIA

Is the allocation of tasks described above adequate to ensure the effective achievement of the goals of the PAIA? The answer is no. Litigation is self-evidently too inaccessible and cumbersome to be an effective means to enforce the freedom of information rights in the Act and in the Constitution. This point was accepted by the report of the Asmal Committee, an ad hoc Committee of Parliament chaired by Professor Kader Asmal MP that was tasked with reviewing the performance of the so-called Chapter 9 institutions, ie the various 'State institutions supporting constitutional democracy' established by the Constitution.[41] Reviewing the performance of the SAHRC, the Committee accepted the Commission's own view that 'the cost and complexity . . . [of the PAIA's internal appeals and litigation scheme] often make it difficult if not impossible for individuals or groups to exercise their right to information through the Act. It is significant that only a handful of cases reach the courts'.[42] The Committee heard no evidence that the powers of the SAHRC to assist requesters been used to ameliorate this problem.[43] Moreover, as for the SAHRC's promotional duties in relation to the Act, there was little to suggest that the Commission had had much success in this regard. The Committee noted a 'lack of knowledge by public servants and private bodies of the provisions of the Act', commenting that, given that it was the task of the SAHRC to educate the body of information-holders about their duties, that 'this lack of knowledge points to a failure on . . . [the Commission's] part'.[44]

The Asmal Committee's conclusions support widely-held perceptions that the enforcement provisions of the PAIA are deficient in two respects:

40 In terms of the Federal Freedom of Information Act 1982, complaints about procedural failures are investigated by the Commonwealth Ombudsman. Appeals against refusals of requests are made to the Administrative Appeal Tribunal.

41 Parliament of the Republic of South Africa *Report of the Ad Hoc Committee on the Review of Chapter 9 and Associated Institutions* (2007), <http://www.parliament.gov.za/live/chapter_9_report.pdf> (Asmal Committee Report).

42 Ibid 174.

43 Ibid.

44 Ibid. The Asmal Committee's conclusions correspond to independent research conducted by an NGO, the Open Democracy Advice Centre (ODAC), which showed that PAIA requests to both the public and private-sector were dealt with extremely slowly or, more troublingly, simply ignored. Open Democracy Advice Centre 'Southern Africa Summary Country Report: Open Society Institute Justice Initiative: 2004 Monitoring Study', <http://www.opendemocracy.org.za/documents/SA2004OSJIMonitoringStudySummaryRTKday.doc>. There appears to be widespread ignorance of the requirements of the Act, even of its existence, in the public sector. An earlier survey conducted by ODAC revealed that 54 percent of the public bodies contacted by the Centre were unaware of the Act, 16 percent were aware of the Act but did not implement it and only 30 percent were aware of it and implementing it. "Few Groups Aware of Act on Access to Information," *Business Day*, October 14, 2002.

- For the extensive rights of access to information granted by the PAIA to be more than rights on paper, provision must be made for resolution of access disputes by some form of independent tribunal. The tribunal must be easily accessible and it must be able to decide disputes authoritatively, cheaply, quickly and effectively. Because of the expense and inefficiencies associated with litigation in the ordinary courts, most jurisdictions opt for dispute-resolution by a specialised information Commission or by specialised administrative tribunals.
- For access to information to succeed in its goals of securing an open and transparent democracy, it is essential that citizens know of their rights under the Act and that officials know about their duties under the Act. This requires mechanisms to be put in place for educating the public about the Act and training officials in responding to requests. Promotion of the goals of the Act also requires mechanisms for assisting members of the public to make requests. Provision should be made for compiling statistics on the use made of the Act with the aim of identifying and remedying defects in the legislation and/or in official compliance with it. Again, most jurisdictions impose these tasks on a specialised information commission.

The Committee's recommendations to correct these problems centred on the creation of an independent 'dedicated information commissioner' with power to 'receive appeals from persons lodging requests for information and make binding orders on access and disclosure'.[45] For reasons of cost, the Committee did not support the SAHRC's own recommendation that an entirely new institution be established to perform these functions, but rather recommended the appointment of an information commissioner within the SAHRC with a 'ring-fenced' budget and a dedicated staff.[46]

The Asmal Committee's recommendations do not consider the Law Reform Commission's proposals for a new information protection authority with enforcement authority over both the PAIA and the proposed data protection legislation. It is to those proposals that we now turn.

III THE LAW REFORM COMMISSION'S PROPOSALS

(a) The EU requirements on data protection enforcement measures

Against the background outlined above, the recommendations of the Law Reform Commission for a 'joined-up' specialised regulatory authority responsible for data protection and for access to information are extremely promising and should be supported. The principal influence on the Commission's recom-

45 Asmal Committee Report (note 41 above) 174.

46 Ibid 174—5. The Committee made no reference to the Law Reform Commission's proposals for a separate information protection authority. The Committee also made recommendations for the merger of several of the current Chapter 9 institutions with a human-rights mandate (specifically the SAHRC, the National Youth Commission, the Commission for the Promotion and Protection of Cultural, Religious and Linguistic Communities and the Pan South African Language Board) into an 'umbrella human rights body to be called the South African Commission on Human Rights' (ibid xii).

mendations in this regard is the European Union's data protection regime, a regime set out in the 1995 Data Protection Directive (EU Directive).[47] The reason for the Directive's extraordinary degree of influence on jurisdictions outside Europe is trade-related: the result of its requirements governing the transfer of personal information to 'third countries' (ie, states outside the European Union). Article 25 of the Directive provides that 'the transfer to a third country of personal data … may take place only if … the third country in question ensures an adequate level of protection'.

As a starting point, 'adequacy' can be taken to mean equivalence; in other words, personal data can safely be transferred to a third state if it provides legal protection that is roughly the equivalent of the EU regime.[48] But that is not the only criterion: the level of adequacy of protection 'shall be assessed in the light of all the circumstances surrounding a data transfer or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country'.[49] The European Commission may make binding determinations on the adequacy of protection provided by third countries, pursuant to art 25(6) of the Directive. The effect of such a decision is that personal data can flow from the 25 EU member states and three EEA member countries (Norway, Liechtenstein and Iceland) to a third country that is the subject of an adequacy decision without the need for any further specific safeguards.[50]

The EU's Working Party on Data Protection, set up to advise the Commission about the level of protection in the European Union and third countries, has taken the view that the concept of 'adequacy' requires that privacy protection must not only be adequate in terms of the substance of data protection rules, but in the means for ensuring effective application of those rules.[51] According to the Working Party, an effective data protection system has three components: 1) compliance with the rules must be ensured by making data subjects and controllers aware of their rights and duties and by the presence of effective sanctions for breach of the rules; 2) individuals must be able to enforce their rights rapidly and effectively and without prohibitive cost by approaching an independent institution; 3) individuals must be able to

47 Note 5 above.

48 Bygrave (note 5 above) 80.

49 Article 25(2) of the EU Directive (note 5 above).

50 In the absence of an adequacy finding, it is necessary to provide specific protection by means of a contract between the data transferor and the recipient. In this regard, the European Commission has issued standard contractual clauses for data transfers to third countries: see <http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm>.

51 European Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data 'Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' (1998) ('Working Document 12') 5.

obtain appropriate redress for breach of the rules, including compensation, by recourse to a system of independent adjudication or arbitration.[52]

In Europe (and in jurisdictions influenced by the European model) there is broad agreement that these components of an effective data protection system are best supplied by setting up an independent data protection authority. The EU Directive requires member states of the Union to establish or appoint one or more independent public authorities which are responsible for monitoring the application of the data protection laws adopted by that state.[53] The Directive requires data protection authorities to have investigative powers, powers of intervention, and power to engage in legal proceedings;[54] individuals aggrieved by a breach of the rules must be able to approach the authority for a resolution;[55] the exercise of the authority's powers must be subject to judicial appeal,[56] and authorities must be consulted in developing administrative measures or regulations.[57]

Additional guidance can be gleaned from the standard wording of European Commission adequacy decisions pursuant to art 25 of the Directive. Assessments of adequacy state the principle that:

> Given the different approaches to data protection in third countries, the adequacy assessment should be carried out, and any decision based on Article 25(6) of [the EU Directive] should be made and enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail…[58].

Accordingly, the protection afforded by third-country jurisdictions, in particular those who been subject to a decision of adequacy, provide a useful basis of comparison for the evaluation of the Law Reform Commission's proposals.[59] While there are a limited number of decisions concerning the adequacy of supervisory authorities and implementation of third parties, some pertinent examples will be considered below.

(b) The Information Protection Regulator

Chapter 5 of the draft POPIA of the Law Reform Commission deals with 'Supervision' and proposes the establishment of an Information Protection

52 Ibid 7.
53 Article 28(1) of the EU Directive (note 5 above).
54 Ibid art 28(3).
55 Ibid art 28(4).
56 Ibid art 28(3).
57 Ibid art 28(2).
58 See, for example, Recital 4 of the European Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, 26 July 2000, at <http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm>.
59 The Commission has so far recognised Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection. See 'Commission decisions on the adequacy of the protection of personal data in third countries' at <http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm>.

Regulator. The organisation, functions, powers and procedures of the Regulator have been drafted with the specific requirements of the EU Directive and guiding material in mind. In what follows we briefly (and, given that the proposals have not been finalised, provisionally) examine the proposals against the background of the specific requirements set out in the EU Directive, the objectives identified by the Working Party and the experience of third-party jurisdictions by asking the following questions:

1. Is the Regulator independent?
2. Do the powers of the Regulator foster compliance with rules?
3. Are the Regulator's procedures accessible, rapid, efficient and cost effective?
4. Does the Regulator have strong investigative and intervention powers?
5. Are data subjects afforded adequate remedies?

(i) Independence of the Regulator

The EU Directive requires supervisory authorities to act with 'complete independence',[60] a necessary quality for an institution that will regulate the processing of person information by both the state and the private sector.[61] The import of the adjective 'complete' is that even a small chance of exertion of influence by the state, or bias in exercise of power by the authority, would lead to an inadequacy finding by the European Commission.[62] The requirement of independence from the state is, according to Bygrave, measured by 'the capacity for a data protection authority to arrive at its own decision in a concrete case without being given case-specific instructions…as to what line it should take'.[63] Bygrave goes on to state that ' "complete independence" means that great care must be taken in ensuring that the authorities' inevitable administrative dependence on other bodies (eg, through budget and personnel allocations) does not undermine the functional independence they are otherwise supposed to have'.[64]

The draft POPIA, following the Constitutional convention, states that the Regulator 'is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers

60 See Recital 62 of the EU Directive (note 5 above): 'the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data'; see, further, art 28(1).

61 The draft POPIA applies to the processing of personal information by a 'responsible party'. The latter term is defined as 'a public or private body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal information' (clause 1 sv 'responsible party'). The definitions of 'public body' and 'private body' are the same as those in the PAIA, with the effect that the draft Act is intended to bind the state. On the meaning of 'public' and 'private body', see Currie & Klaaren (note 16 above) [4.7]—[4.13].

62 Bygrave (note 5 above) 71.

63 Ibid 70.

64 Ibid 71.

without fear, favour or prejudice'.[65] But such a declaration cannot overcome any procedural and structural deficiencies in the legislation's design that detract from independence. In this regard, the Asmal Committee's review of the Chapter 9 institutions has provided useful guidance on important institutional aspects of independence. Taking as a starting-point the constitutional standard of independence, ie whether from the standpoint of a reasonable and informed person there is a perception that an institution is independent,[66] the Committee concluded that the relevant factors for assessing the independence of a rights-protecting or regulatory institution are the following: 'financial independence; institutional independence with respect to matters directly related to the exercise of its constitutional mandate, especially relating to the institution's control over the administrative decisions that bear directly and immediately on the exercise of its constitutional mandate; appointments procedures and security of tenure of appointed office bearers'.[67] In relation to all of these factors, institutions must 'manifestly be seen to be outside government'.[68] This means that the National Assembly and not the executive is the appropriate body to oversee the appointment of members, financial matters such as budgets, and it is the Assembly to which independent institutions should account.[69]

The published draft recommendations of the Law Reform Commission[70] in relation to the factors just mentioned lack detail and are clearly deficient when measured against the precise standards outlined. However, these are preliminary proposals which the Commission clearly intends to flesh out and modify in its final report. In doing so, it will undoubtedly be guided by the Asmal Committee's recommendations on institutional, financial and administrative independence, particularly with regard to the necessity of Parliamentary rather than executive control and accountability. If so, the result should be a data protection authority that meets both the EU standard of independence[71] and that of the Constitution.

65 Clause 35. The formulation follows the establishing clause of the Chapter 9 institutions: s 181(2) of the Constitution.

66 *Van Rooyen v S* 2002 (5) SA 246 (CC) paras 32-4.

67 Asmal Committee Report (note 41 above) 9-10.

68 *Independent Electoral Commission v Langeberg Municipality* 2001 (3) SA 925 (CC) para 31.

69 Asmal Committee Report (note 41 above) 10.

70 Note 1 above.

71 For example, in the United Kingdom the Information Commissioner, who is responsible for implementing and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000 is appointed for a five-year term by the Queen on the recommendation of the Minister of Constitutional Development but can, however, only be removed by Parliament. See Schedule 5 to the Data Protection Act. Both the Privacy Commissioner and the Information Commissioner in Canada are appointed on the recommendation of Parliament for a seven-year term and can only be removed by Parliament. See 1980-81-82-83, c 111, Sch II s 53 of the Privacy Act 1980. By contrast, Slovakia, which became a member of the EU in 2004, was required by the European Commission to make changes to the legislation governing its data protection authority to ensure that it would be able to 'carry out its functions fully independently, not just from executive power but also from any other state authorities', particularly with respect to the allocation and disbursement of its budget and appointment of staff. See Working Party on the Protection of Individuals with regard to the Processing of Personal Data *Annual Report 2004*, 82 <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/8th_annual_report_en.pdf>.

It is intended that the Regulator's mandate should include promotional, advisory, mediation and enforcement functions. It is worth noting that it will be necessary to create mechanisms to ensure that these functions can be carried out independently of each other. To ensure impartiality, employees or members of the Regulator responsible for advice, mediation or investigation should also not have the power to make binding orders.[72]

(ii) Fostering compliance with rules

The EU Directive requires data protection authorities to be consulted when 'drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data',[73] and requires authorities to report publicly on their activities at regular intervals.[74] According to the Working Party, these provisions support the objective of fostering compliance with data protection rules by ensuring a high degree of awareness of data controllers of their obligations, and among data subjects of their rights and means of exercising them.[75]

The draft POPIA specifically requires that the Regulator is consulted in the development of regulations and industry codes of conduct, and more generally, it is intended that the Regulator will have an educational and promotional mandate.[76] As to reporting, the model of the Chapter 9 institutions, set out in s 181(5) of the Constitution, is appropriate for the Regulator and should be followed: bodies 'are accountable to the National Assembly and must report on their function to the Assembly at least once a year'.[77]

(iii) Accessible, rapid, efficient and cost-effective enforcement of rights

As the experience of the PAIA vividly illustrates, legislative rights have limited effectiveness unless a supervisory body has the capacity to provide accessible, rapid, efficient and cost-effective means for individuals to enforce those rights. In this regard, the proposals for the proposed Information Protection Regulator to have binding dispute-resolution powers and to exercise these powers in respect of both the POPIA and the PAIA are crucial. These powers are necessary not only to the success of the proposed data protection regime but are also an opportunity to cure the single most problematic aspect of the access to information regime created by the PAIA.

In essence, the draft POPIA proposes that individual data subjects may approach the Regulator for assist in the enforcement of their rights. In the case

72 In other jurisdictions, for example the United Kingdom, enforcement functions are allocated to a tribunal, which operates separately from and independent of the data protection authority itself.

73 Article 28(2) of the EU Directive (note 5 above).

74 Ibid art 28(5).

75 Note 51 above.

76 Note 1 above, chapter 5 of the Draft Bill.

77 The Asmal Committee made several recommendations to improve the exercise by Parliament of its accountability and oversight functions over the Chapter 9 institutions. Most notably, it recommends the creation of a co-ordinating Unit on Constitutional Institutions and Other Statutory Bodies, located in the Speaker's office. See Asmal Committee Report (note 41 above) 30-31.

of the POPIA, these rights stem from the list of 'Conditions for the Processing of Personal Information' in Chapter 3 or from an industry-specific Code of Conduct issued by the Regulator in terms of Chapter 7. In the case of the PAIA, the rights stem from the right to request access to a record in s 11 and s 50. On receipt of a complaint, the Regulator must investigate (it has powers of compulsion of evidence to assist it, see part (iv) below), may attempt to settle the dispute or may make a binding decision on the complaint, called an 'enforcement notice'. An aggrieved party may appeal an enforcement notice to the High Court within thirty days of its issue. The enforcement powers of the Regulator do not include the award of financial penalties, but a data subject may apply to the High Court for an award of damages resulting from an infringement of statutory rights and may request the assistance of the Regulator in making such an application.

Currently, the draft POPIA provides little detail on time periods for the settlement of disputes. This aspect, which goes to the goals of rapid and efficient enforcement of rights, should not be neglected and the final legislation or internal regulations should specify time periods for the processes of investigation, assessment, and issuing of enforcement notices.[78]

(iv) Investigative powers

The EU Directive provides specific details regarding what constitutes effective investigative and intervention powers for data protection authorities, powers that are vital for the effective regulation of the statutory rights.[79] The draft POPIA proposes that the Regulator will have powers to collect evidence required to investigate complaints and of search and seizure and, in accordance with the proposal that the Regulator also has powers to enforce the PAIA, these should also apply to investigation of access to information matters.

(v) Redress and remedies

As we have seen, the Working Party has identified that a primary objective of the enforcement provisions of a data protection regime must be to provide appropriate redress through independent adjudication or arbitration, allowing compensation to be paid and sanctions imposed where appropriate. The EU Directive more specifically requires that data subjects have a right to judicial remedy,[80] that decisions of an authority giving rise to complaints must be

78 A pertinent example of the importance of such requirements is found in the case of New Zealand, which fell short of providing an adequate level of protection partly due to the inability of its Privacy Commissioner to finalise complaints within a reasonable time. It was reported that the 'EU consultants who conducted an adequacy survey on New Zealand expressed concern that a delay of 14 months in finalising complaints was highly disturbing'. Phukubje Pierce Masithela Attorneys 'Meeting EU standards on data transfer' 1503 *Legalbrief Today*, 18 January 2006.

79 Article 28(3) of the EU Directive (note 5 above).

80 Article 22 of the EU Directive (ibid).

appealable through the courts, and that authorities must have the power to engage in legal proceedings.[81]

The binding enforcement notices to be issued by the Regulator will provide an important mechanism for redress for data subjects.[82] This power is somewhat diluted by the fact that the Regulator, unlike some other jurisdictions,[83] lacks authority to award compensation or impose fines.[84] Data subjects are required instead to institute court proceedings to obtain compensation, thereby detracting from the objective of the Commission to be a rapid, efficient and accessible dispute-resolution mechanism. It is intended that the Commission will have the power to institute court proceedings to recover damages on its own initiative or at the request of data subjects. This will go some way to curing the problem just mentioned but only if the Regulator has the capacity to provide such assistance for every data subject who is seeking compensation.

In relation to appeals, the current draft of the POPIA provides a right of appeal to the High Court to the person upon whom an enforcement notice has been served, but is silent about data subjects' right of appeal against the content of the notice or a decision not to issue one. The current lack of an express right of appeal is a significant inadequacy in compliance with arts 22 and 28(3) of the EU Directive and should be rectified in the final version of the proposed legislation.

IV Conclusion

The experience of the inadequate enforcement of the PAIA shows that a statutory rights regime is likely to be ineffective unless adequate, accessible and cost-effective mechanisms are provided to right-holders to allow them to enforce their rights. The necessity for a proposed statutory regime for the protection of privacy rights in relation to personal information to comply with the EU framework, a framework that places considerable emphasis on effective enforcement of data protection rights, is therefore salutary. The demands of ensuring that the South African data protection regime provides an 'adequate level of protection' will ensure that the resultant legislation does not suffer from the same design flaws as the PAIA, flaws that, as we have seen, had their origins in the enforcement provisions of the Open Democracy Bill. At the same time, the Law Reform Commission's proposals that the principal enforcement institution of the POPIA — the Information Protection Regulator — should have corresponding powers to enforce compliance with the PAIA, have the prospect of curing many of the PAIA's current defects. Moreover, given the considerable degree of overlap between the functions of data protection and

81 Ibid article 28(3).

82 See the discussion in part (ii) above.

83 For example, the Privacy Commission of Australia, which has the power to award compensation or impose fines.

84 The EU Directive and interpretative materials do not specifically require that the right to compensation be enforced by bodies other than courts, and it appears recovery of compensatory damages can be provided as either a judicial or administrative remedy. G Greenleaf 'The European Privacy Directive — Completed' (1995) 2 *Privacy Law & Policy Reporter* 81.

access to information, the institutional design of the proposed Regulator — a subject-specialised regulatory authority, necessarily equipped with considerable technical expertise in fields such as information systems and information security — is highly appropriate for supervision of the PAIA.

The Law Reform Commission's published proposals provide little detail on the mechanics of the enforcement of the PAIA by an Information Protection Regulator. This is because the proposals were intended principally to canvass opinion on the merits in principle of creating a joint regulatory authority to supervise data protection and access to information. Though the technical difficulties of merging the enforcement provisions of the two statutes should not be underestimated, we have attempted to show here that the proposal has a great deal of merit, that the result should be the effective protection of the constitutional rights to privacy and access to information and that it should be supported.

Kate Allan
Freedom of Information Project Co-Ordinator,
South African History Archive

Iain Currie*
Professor of Law, University of the Witwatersrand, Johannesburg

* Iain Currie is a member of the South African Law Reform Commission's project committee on Privacy and Data Protection. The views expressed in this note should not be attributed to the Commission or the project committee.