South Africa edges towards data protection legislation

The South African government is expected to publish a draft data protection bill by the end of this year, although when legislation will finally be passed is still unclear. **James Michael** outlines the developments and suggests that demands from the European outsourcing sector could provide the incentive to move forward.

Although South Africa's data protection legislation was supposed to be simultaneous with freedom of information, the Promotion of Access to Information Act became law in 2001, while data protection will only reach the stage of a draft bill at the end of 2004.

Data protection originally had been more closely connected with freedom of information legislation than in most countries (but not all, eg. France and Canada's nearly simultaneous national access to information and privacy laws). It started with the Interim Constitution in 1993 which became, with modifications, the Constitution in 1996. Both the Interim and the final Constitutions had provisions establishing the right to personal privacy. They also both had provisions establishing the public right of access to information.

During the Mandela presidency (1994-1999) there was an inquiry into the related questions of access to government information and privacy. Instead of being referred to the South African Law Commission (now the South African Law Reform Commission) the matter was referred to a committee chaired by the then-Deputy President, and now President, Thabo Mbeki.

They reported in 1996 with the Open Democracy Bill, which was introduced into Parliament in 1998, withdrawn, and re-introduced in 1999. The bill included four parts: one establishing a public right of access to information, the second establishing open meeting rules, the third providing protection for disclosures in the public interest, and the fourth providing privacy protection for personal information under government control.

The constitutional right of access to information had been interpreted by the Constitutional Court as requiring the constitutional provision to take direct effect if implementing legislation was not law by February 3rd 2000. In December 1999 it became obvious that the Open Democracy Bill could not complete all the parliamentary stages by February, and the whistleblower protection, open meetings, and privacy protection sections were removed so the access to information section could become law by the deadline. The whistleblower protection section later became law as the Protected Disclosures Act 2000. The original privacy protection section was not really a data protection law in the sense of the Council of Europe Convention or the EU Data Protection Directive, being closer to the original US and Canadian Privacy Acts. So, the government started over again on data protection.

> The timing of the data protection bill could well be influenced, as it has been in India, by the growth of information technology outsourcing in South Africa from Europe.

Privacy consultation

The subject of privacy and data protection was referred to the South African Law Commission in 2002, which appointed a committee to consider the matter (Project 124). In August 2003, the committee published its Issue Paper and asked for comments by the beginning of December 2003. They are now examining the comments received and will publish a further Discussion Paper, including a draft bill, around the end of 2004. The Issue Paper reviews the history and theory of privacy law, considering common law protection in South Africa through the general civil remedy for invasion of privacy and other related wrongs, and the Constitutional protection.

Data protection is described in terms of international measures and national legislation, including the Council of Europe Convention, the OECD Guidelines on privacy, the EU Directive, the UN Guidelines, and the Commonwealth Model Bills. National legislation is noted, including subject access under the Promotion of Access to Information Act, and encouragement of voluntary data protection under the Electronic Communications and Transactions Act.

Approaches to data protection regulation

The paper identifies four models of data protection: comprehensive laws, sectoral laws, self-regulation, and technology. The Commission emphasises that: "It is clear that the process of establishing policy goes beyond the level of basic statutory data protection principles to include the ways in which these principles should be enforced, eg.

through supervisory authorities."

As a starting point the Commission proposes that the next stage of the investigation should include automatic and manual files, information about both natural and legal persons, information kept by both the public and private sector, and both sound and image data. The inclusion of information about both natural and legal persons (ie. companies) is because of the limited recognition in South African case law of a corporate privacy right. Extension of data protection legislation in South Africa to legal persons would be unusual, but not unprecedented.

OUTSOURCING IS AN INCENTIVE

The question of when that bill will be introduced and when it is likely to become law is a matter of political priorities. The timing of the data protection bill could well be influenced, as it has been in India, by the growth of information technology outsourcing in South Africa from Europe. Call centres, for example, have been growing rapidly in the past few years in South Africa, aided by an Anglophone and IT-literate population, the same time zone as Europe, and a low wage economy.

If the EU Data Protection Working Party turns its attention to examining whether data protection in South Africa is 'adequate' in terms of the EU Directive, it could be a significant incentive to rapid legislation. Thus far, the Working Party has made adequacy findings on Switzerland, Hungary, Canada, the US Department of Commerce Safe Harbor Principles, and Argentina, with Australia and New Zealand heading its programme of work for 2004.

AUTHOR: James Michael is a Senior Research Fellow for the Institute of Advanced Legal Studies, London University, and a professor at the University of Cape Town.

India commits to data protection, continued from p.3

EU than it does with the US and that its population is around three times larger than that of the US. But it is doubtful that the European Commission will devote the time and resources needed to pursue this option. One reason is that a safe harbor agreement with India could spark off requests for similar arrangements with several other countries. In any event, critics of the safe harbor arrangement argue that it is a poor substitute for a law.

4. Amend the IT Act - Acharya explained that India's IT Act 2000 addresses utilisation of IT, covering issues such as hacking and other forms of cybercrime. Section 43 of the law makes provision for claiming up to 10 million Rupees ($225,000, €190,000) in compensation for breach of the law. It would be possible to add an amendment to cover data protection.

Pavan Duggal, who drafted the IT Act, explained to *PL&B International* that the IT Act has three main objectives:

- legalise business conducted electronically
- facilitate e-filing of documents with government agencies; and
- provide consequential amendments to certain other laws, such as the Penal Code and the Evidence Act.

For the first time in India, this law provides a definition of "data" and "information" and so provides a convenient existing vehicle for a new data protection section.

5. A Data Protection Ordinance - Duggal explained that a further option for the government is to adopt a Data Protection Ordinance. The advantage is that it could be introduced with immediate effect. The disadvantage is that it would need to be ratified by both houses of the legislature within six months, otherwise it would cease to have effect. Such an outcome would be embarrassing for the government. A further disadvantage is that data protection is not a subject which requires such immediate action. It would be better to achieve consensus and support from the interested parties. This approach would be more likely to work effectively in practice.

6. A specific data protection law for the private sector - There is little support for this option because there is no perceived need in India from the business perspective. Another problem with this option is that it would take valuable and scarce parliamentary time to introduce such a law and could take up to two years to pass through all its legislative stages.

Whichever option emerges from this process, it is unlikely to follow any existing national model. Instead, it would need to address the specific Indian context. Any data protection initiative would not be aimed at the domestic context but rather the business process outsourcing sector.

Questions which the IT Ministry's advisory committee will need to address include:

1. If the government goes ahead with any of the data protection proposals, it needs to consider whether it would use current or new oversight and enforcement agencies.

2. Would the compensation provisions of the IT Act be extended to breaches of individuals' privacy or data protection 'rights'?

Both Duggal and Acharya expect more clarity on the government's way forward to emerge soon after the forthcoming election. The CII's Acharya summarised the consensus of all domestic parties to India's data protection debate. "Economic growth is vital to the mass of India's population. Nothing should be done to harm that growth."

KEY CONTACTS: Pavan Duggal Associates, New Delhi, India (E-mail: pduggal@nde.vsnl.net.in; Website: www.cyberlaw.net)

Anindya Acharya, Deputy Director for IT, Business Process Outsourcing and E-Commerce at the CII can be contacted at: anindya.acharya@ciionline.org

For details on India's IT Act 2000, visit the Ministry of IT website at: www.mit.gov.in