POPI – Is South Africa keeping up with international trends?

By Russel Luck

In South Africa, the much anticipated Protection of Personal Information Act 4 of 2013 (POPI) was promulgated in Gen 912 *GG* 37067/26-11-2013. Its commencement date shall be determined in accordance with s 115 of POPI by the President and its provisions will come into effect one year thereafter.

What is the paradigm of personal information and privacy legislation?

The internet allows data transactions to occur from one country to another seamlessly. Paradoxically, this is one of the greatest benefits of the technology era but also one of the greatest challenges to its effective regulation. Citizens bound by data privacy laws in their country could transfer data to countries that are less regulated than their own and by-pass the protection that is offered by that state to its citizens.

European Union laws such as European Union Data Protection Directives of 1995 ((23-22-95) Official Journal of the European Committees No 281/31), 2002 (OJ L 201, 31.7.2002, p 37) and 2006 ((13.4.2006) Official Journal of the European Union L 105/54) (the EUDPD) have been highly influential on the drafters of POPI. A detailed discussion is beyond the scope of this article, save for mentioning that the EUDPD aims in art 1 to provide for economic and social progress of European Union (EU) members and art 25 prohibits transborder information flows to countries with less data privacy protection than member states. The EUDPD has been successful in creating uniform standards of data privacy for all member states with the result that businesses within the EU that are reliant on data can easily transact with one another. This, in turn, has assisted economic and social progress among signatories of the EUDPD.

The challenge arises when EU members conduct business in jurisdictions that have less data privacy regulation than their own. Article 25 of the EUDPD prohibits data transfers necessary for such business to occur. The United States (US) has not adopted uniform data protection standards equivalent to the EUDPD. Data-reliant industries such as direct marketing, insurance, banking, travel, finance and pharmaceuticals all rely on data profiles in order to operate business. Should European businesses wish to transact with US companies and gain the economic and social progress mentioned in art 1 of the EUDPD, art 25 of the EUDPD prevents them from doing so.

Ostensibly, the US adopted the United States Department of Commerce Safe Harbor Privacy Principles 2000 (Safe Harbor Agreement) that allow US businesses to self-certify that they are compliant with the standards of data protection adopted by EU nations through the EUDPD. The problem with self-certification is obvious, there is very little practical control or enforcement the EU citizens would have over American companies who received their personal information. According to the Safe Harbour Decision Implementation Study (http://export.gov/safeharbor/eu/eg_main018475.asp, accessed 11-4-2014) conducted in 2004, a prevalent minority of US entities complied with EUDPD principles. Non-compliance ranged from lack of privacy policy displayed on websites to lack of clarity regarding ‘onwards transfers’ of data and disclosing the ‘intended use’ of processing that data.

It appears that the current paradigm of personal information legislation is that individual privacy seems to rank below the economic interests of global business. This international paradigm is important when understanding how POPI might be interpreted by our courts and function practically in the global economy.

How does POPI balance the international privacy paradigm?

POPI was drafted largely on the recommendations of the South African Law Reform Commission (SALRC) in discussion paper 109 of project 124 (2005) (www.justice.gov.za/salrc/dpapers/dp124.pdf, accessed 11-4-2014). The SALRC expressly recognised the importance of privacy in terms of the constitution and pre-existing common law. It noted that while privacy is a fundamental right, it can be limited and balanced against economic and trade considerations looking at data privacy not only as a domestic policy issue but as part of the global community. A comprehensive analysis of POPI is beyond the scope of this article. Some of POPI's key features are dealt with below:

• POPI will affect many industries across South Africa, finance, insurance, pharmaceuticals, direct marketing and retail are just some of the sectors that will need to make adjustments in order to be POPI compliant. Much like Regulation of Interception of Communication-related Information Act (RICA) 70 of 2002, which was supplemented by a directive, notice, schedule, four proclamations and two amendments (with a further two amendments pending), POPI will most likely undergo changes in the future. It is improbable that each and every outcome of POPI could be foreseen by the drafters at inception of the Act. It is probably for this reason that POPI provides for an information regulator defined as the 'Regulator' who will, among other things, report to parliament on issues relating to POPI and be responsible for 'codes of conduct' that will set obligations and conditions for the lawful 'processing' of 'personal information' (ss1, 34, 60 – 68 of POPI). POPI's commencement date has yet to be determined by the President and its provisions become effective one year thereafter. This grace period will provide time, perhaps not enough, for affected parties to make certain adjustments and communicate with the 'Regulator' on issues specific to their industry.

• POPI regulates the 'processing' of personal information. The definition of 'processing' is very wide and refers to almost any instance where personal information is handled. The scope of POPI is narrowed by the definition of personal information that lists many types of information considered to be personal information. This definition is not a closed list and even information not listed in s 1 as personal information could be considered personal information and protected by POPI. Personal information is not information that is 'de-identified' or information that relates to a purely personal or household activity. There are further exclusions for journalistic, literary or artistic expression and matters of national security. The gateway into POPI lies inside the ambit of personal information and 'special personal information' but outside the ambit of anything that is considered de-identified or exempt. Information that has been 're-identified' no longer falls outside the ambit of POPI and would be protected by the Act.

• POPI confers rights on 'data subjects' including but not limited to, the right to be notified when personal information is processed and the right to be notified when personal information has been compromised or hacked by unauthorised individuals. Data subjects have the right to know (free of charge) if a 'responsible party' holds the personal information of a data subject. They also have the right to a record or copy of that personal information but the responsible party may charge a fee for providing access to this record. Data subjects have the right to correct and amend the records of their personal information held by responsible parties. They also have the right to object to the processing of their personal information and not to be subjected to direct marketing. The rights of data subjects is not absolute under POPI and can be limited where, for example, providing access to a record would defeat the object of that record or the information regulator has provided an exemption to the responsible party under POPI.

• Conversely, POPI confers duties on responsible parties to 'process' personal information in compliance with conditions, including but not limited to, the condition that processing must be conducted in a manner that is accountable, lawful, reasonable and has a minimal intrusion on the data subject's rights. Personal information processing (under normal circumstances) must be done with the consent of the data subject and gathered from the subject directly, though this is not the only way personal information can be processed. Personal information must be collected for a specific purpose and the data subject must (under normal circumstances) be notified that their personal information is being processed. There are limitations on the length of time personal information can be retained. There are also limitations on processing personal information for reasons other than those disclosed to the data subject. Personal information must be reasonably accurate and secure from unlawful access and further dissemination.

• ‘Operators’ or people acting under contract or mandate of a responsible party have a duty not to disclose any personal information they come into contact with and must maintain the integrity and confidentiality of the personal information they have collected.
• One of the issues raised by practitioners and mooted by parties affected by POPI is whether POPI applies retrospectively (www.pmg.org.za/report/20130522-protection-personal-information-bill-departmental-and-public-representations, accessed 2-4-2014). One of the concerns is that immediately prior to POPI coming into force, a surge of personal information may be transferred in a final attempt to compile precious databases for marketing and business purposes. POPI in its current form does not apply retrospectively and in the absence of the Act being amended or the President bringing it into force with retrospective effect, this position will stand. It is my view that POPI would be too large a burden to administer and enforce retrospectively. Moreover the consent and opt-out provisions under s 69 of POPI would provide data subjects with sufficient ability to curtail unsolicited marketing communications relatively quickly.
• Once POPI is in full force and effect penalties for non-compliance are severe, amounting to fines not exceeding R 10 million or imprisonment of up to ten years (ss 107 and 108 of POPI). POPI’s provisions are onerous and expansive. Compliance is not a one-size-fits-all matter and each business will require its data practices and data privacy policies to be reviewed by their respective legal advisers.
• Lastly, like art 25 of the EUDPD, s 72 of POPI prohibits transborder data flows to countries that have lower standards of data protection than South Africa. This affects the ability of South African businesses to transfer information in the global market place. It does, however, allow South African businesses to receive data flows from countries that have similar data protection provisions in their jurisdiction. Had POPI not been drafted with a limitation on transborder data flows, South African businesses would struggle to transact with businesses based in the EU. In cases where South African businesses wish to engage in transborder data flows to countries that have lower data protection standards than South Africa, obtaining the data subject’s consent or satisfying another exception to s 72’s prohibitions would ease restrictions on South African businesses from engaging in transborder data flows to businesses in those jurisdictions.

Challenges and analysis
Technology evolves faster than law makers can regulate it

A recent incident in the US demonstrates the need for data protection and the manner in which current practices ‘fudge’ technology matters regulated by statute. *The Wall Street Journal* reported (Dana Mattioli ‘On Orbitz, Mac Users Steered to Pricier Hotels’ *The Wall Street Journal* 23-8-2012, (http://online.wsj.com/news/articles/SB10001424052702304458604577488822667325882, accessed 2-4-2014)) that a search engine powered by Orbitz Worldwide Inc suggested more expensive hotels to users visiting the site with a Mac Computer than a personal computer.

The details relating to this scandal are varied and it is not clear what information was processed by Orbitz. It was traditionally believed that an internet protocol (IP) address is not ‘Personally Identifiable Information’ (American definition) because it relied on a dial-up connection to access the internet, each time a user dialed-up, a new IP address was assigned to that computer. However, according to PM Schwartz and DJ Solve, the mass movement away from dial-up and towards broad-band internet use has resulted in fixed IP addresses being assigned to certain computers as unique identifiers (‘The PII Problem: Privacy and a new concept of personally identifiable information’ (2011) 86 *New York University Law Review* 1814). Whether an IP address reveals a user’s ‘identifying number, symbol … online identifier’ sufficient to trigger subs (*c*) under the ‘personal information’ definition in POPI has yet to be evaluated by our courts. As always, clarity will be established on a case-by-case basis.

In the above, the concept of ‘de-identified personal information’ had its vulnerabilities exposed. In 2006, America Online (AOL) released 20 million search queries for research purposes, which it believed to be sufficiently de-identified. Reporters at the *New York Times* exposed the ease with which such information could be re-identified using techniques that tracked searches for landscape gardeners in a specific area with a host of circumstantial information to reveal the identity of a user.

Clearly technology evolves at a speed that exceeds our law maker’s ability to regulate it in its entirety. It is hoped that the information regulator and industry leaders will dialogue over the provisions of POPI to ensure our system of data protection is coherent and in keeping with current technology practices.

First world laws and third world problems

POPI’s place in the international privacy paradigm is promising. Its provisions match the EUDPD’s standards of data protection with the effect that South African businesses could engage in transactions with European businesses that are heavily reliant on data. What has yet to be seen is whether the US’s standards of data protection will satisfy South Africa in the same way that the EU has accepted the Safe Harbour Agreement despite its imperfections. The SALRC in its discussion paper 109 of project 204 sought to balance the right to privacy against economic and social progress. This aspiration is reflected in the preamble of POPI. South Africa is a developing economy and strives to attract foreign investment that is critical for its future development and growth.

Many of South Africa’s technology industries are in their infancy, despite having solid legal regulations in place. Amazon.com Inc opened its customer service centre in Cape Town in 2010 and software development centre thereafter. It forecasted that 1400 new jobs would be created when operations are at their peak. Similarly, Google Inc’s expansion of its office in Johannesburg is an encouraging sign of foreign business interest in South African opportunities. POPI should be interpreted in a manner that is friendly to foreign business yet protective of unscrupulous information practices. There is every reason to be optimistic that it will achieve both these aspirations.

Russel Luck *BA LLB (UCT)* is a legal adviser in Thailand.