CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

Johannesburg

10 October 2012

TAKING PRIVACY TO THE NEXT LEVEL

What is 'privacy', and why is it important? One of the most challenging aspects of privacy is that it means different things to different people. It was characterised in 1890 by a (then) future United States Supreme Court Justice[1] as the 'right to be let alone', however, this definition is too broad and vague to be usefully applied. Privacy has also been described in terms of guarding that which is 'intimate' about oneself, and yet this definition is too narrow, as much information about oneself may be considered private, and yet not intimate. Perhaps one of the more useful ways of understanding privacy is to think of it as an interrelated and overlapping set of concepts with significant similarities. A prominent US legal scholar has made this argument,[2] and created a taxonomy of privacy encompassing four categories of privacy violations: information collection, information processing, information dissemination, and invasion.

Privacy today is held to be a basic human right, as articulated in the Universal Declaration of Human Rights, and in the Constitution of South Africa. In this context, privacy is viewed as a fundamental element of human dignity and autonomy. Drawing on this perspective, one can understand privacy as the right to be free of observation (or even the fear of observation, which has been demonstrated to alter peoples' behaviours), as well as the right to control the collection, use, retention, and dissemination of information about oneself. Privacy, therefore, in a democratic and free society, has intrinsic social value – and yet, privacy is not an absolute value unto itself. It is a right that must be balanced against other societal needs and values, such as security. If one considers the value of closed-circuit television (CCTV), for example, in public safety, one understands that the sacrifice of personal privacy might under certain circumstances be necessary.

Over the past three decades, privacy has gradually achieved increasing prominence as a business issue, as computer use and the internet have become ubiquitous. In 1980, the Organisation of Economic Cooperation and Development (OECD) adopted 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', which have formed the foundation for international privacy legislation worldwide. The guidelines formalised eight principles that have come to be known as 'fair information practice principles':

- collection limitation: information collected about a person should be limited to that which is necessary for the purpose for which it is collected, should be collected lawfully, and with the person's knowledge or consent;
- data quality: information collected should be relevant to the purpose for collection, and kept up to date, accurate, and complete;
- purpose specification: a person should be informed as to the purpose for the collection of their information at the time of collection, and the uses that will be made of their information;
- use limitation: a person's information should not be used for purposes other than the original purpose without that person's explicit consent or in accordance with law;
- security safeguards: a person's information should be protected;
- openness: collection and use of a person's information should be transparent;
- individual participation: a person should be able to ask if information about them is held, should be able to see that information, and should be able to correct their information or have it deleted; and
- accountability: holders of information should be accountable for the above.

[1] Samuel D. Warren & Louis D. Brandeis 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193–220.
[2] Daniel J. Solove ' "I've Got Nothing To Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745.

PROUDLY SOUTH AFRICAN

One need only look to companies such as Google and Facebook today to understand the business value that personal information now holds. Google and Facebook are able to offer tremendously valuable software services to hundreds of millions of people worldwide 'free of charge', because they are able to collect and use individuals' personal information for commercially profitable purposes.

Beyond business value, personal information has achieved immense value in a vast international criminal underground, trading for as little as US$7 (R51) per record to as much as US$1 000 (R7 349) per record, depending on geography. The online criminal enterprise has evolved way beyond the rebellious teenage hackers of the 1980s to organised crime syndicates and sophisticated criminal attacks targeted at organisations and individuals.

Even more disconcerting is the reality of corporate espionage, and the role of foreign states in cyber-espionage and warfare. The value of an organisation's intellectual property to emerging powers should not be underestimated. Against this backdrop, Bill number 9 of 2009 was introduced in South Africa's Parliament: the Protection of Personal Information Bill (or 'PoPI'). The objective of the Bill is to;

> – regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests

The Bill accomplishes this objective by establishing eight conditions for the lawful processing of personal information (these conditions closely mirror the eight OECD principles described above), and by establishing an Information Regulator that sets standards for the lawful processing of personal information, investigates unlawful processing of personal information, and imposes sanctions (including fines) for unlawful processing. The Bill also endeavours to harmonise existing privacy legislation in the Promotion of Access to Information Act 2 of 2000 (PAIA), the Electronic Communications and Transactions Act 25 of 2002 (ECTA), the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), the National Credit Act 34 of 2005 (NCA), and the Consumer Protection Act 68 of 2008 (CPA).

At the time of writing this article, the Bill has been passed by the parliamentary Portfolio Committee on Justice and Constitutional Development and the National Assembly, and referred to the National Council of Provinces. Once approved, it goes to the President for signature. One of the significant challenges facing organisations is that the Bill currently calls for a one-year implementation time-frame after enactment; however, provision is made for the President to extend the effective date for all or some industry segments, as well as for the Minister to extend the effective date(s) for up to three years after enactment. Most larger organisations would be extremely hard-pressed to implement an effective programme within a year, which is why it is worthwhile to begin such activities now.

While the drafters of the Bill have drawn heavily on existing legislation in Australia, Canada, and Europe, it is in some ways quite different from such comparable laws. Perhaps the most concerning aspect of the Bill lies in its extraordinarily broad definition of personal information. Firstly, personal information is deemed to apply to both natural *and* juristic persons, meaning that the information held about corporate entities (such as vendors and suppliers) is considered to be 'personal information'. Secondly, over forty-five distinct data elements are considered to be personal information, including such esoteric elements as 'personal opinions, views, or preference' and 'the views or opinions of another person about the individual'. When one considers that the Bill covers information in all its forms – spoken, paper and electronic – one begins to realise the magnitude of the impact this will have on South African businesses.

Not only must organisations protect the information of their customers and employees, but they must also do the same for their suppliers and business partners. Notice must be given to these stakeholders of the uses of their personal information. Consent must be obtained, as necessary, and the ability of the party to object must be operationalised. Controls must be established to ensure not only that information is used in accordance with the specified purpose, but also that only the appropriate personnel within the organisation have access to the information and use it for the specified purpose, that the information is kept accurate and up to date, that it is not re-used for any unauthorised purpose, and that it is destroyed when it is no longer needed. Provision must be made for

the individual rights afforded by the Bill, such as requests to receive copies of information and requests to correct or delete information.

While an undertaking such as this might easily be perceived as a regulatory compliance initiative, organisations that view it as such will be missing important opportunities. Firstly, the King Code of Governance for South Africa, 2009 ('King III') correctly identifies that corporate responsibilities extend well beyond shareholder profit. In addition to profit, sound corporate governance extends to people and to 'planet' (integrated reporting covers environmental, social and governance (ESG) matters). In other words, by supporting, upholding, and embracing the fundamental human right to privacy that is enshrined in the South African Constitution and Bill of Rights, South African companies are exemplifying the King principles of good corporate governance and corporate social responsibility.

Additionally, implementing an effective privacy programme can achieve distinct competitive advantages for organisations. South Africa currently has no data breach notification law: however, once PoPI is enacted, companies will be obliged to notify the Regulator and the individual of any misuses or breaches of their personal information. In the United States, for example, breach notification laws were first introduced in 2003, in California, and have led to expansive media coverage of data breaches. In 2009, Heartland Payment Systems set aside US$500 million (R3 695 billion) to cover lawsuits arising from one of the largest known data breaches to date of over 130 million individuals' credit and debit card information. The reputational damage of such press coverage and breach notifications to such vast numbers of people is mind-boggling. By implementing a robust privacy programme, with appropriate information security measures, an organisation can achieve significant advantage over its competitors who fail to recognise and act on such an opportunity.

When one reflects on the Google and Facebook business models, one realises the intrinsic value that customer information holds for companies. One of the aspects of an effective privacy programme is the identification of the nature and whereabouts of the information held within an organisation. By partnering with other key stakeholders within the organisation, the privacy function can become a business enabler by identifying opportunities for efficient and effective information use and flow within an organisation.

The elements of a comprehensive privacy programme parallel those of an effective compliance programme, as defined by the United States Sentencing Commission's Federal Sentencing Guidelines:

1. Accountability: designate an individual in the organisation to be responsible for privacy, and ensure that the individual reports to a senior official;
2. Oversight: ensure that the Board regularly receives reports on and is involved in the privacy programme (see King III);
3. Codes of conduct, policies, and procedures: ensure that these elements are in place within the organisation with respect to privacy;
4. Communications, awareness, and training: ensure that all personnel within the organisation are aware of and trained on their privacy responsibilities;
5. Monitoring and auditing: ensure that the privacy programme is monitored and audited regularly for effectiveness;
6. Enforcement: ensure that policy and procedure violations are sanctioned;
7. Prevention and response: ensure that procedures are in place to prevent and respond to privacy incidents

While many organisations in South Africa will view PoPI as just another onerous, unfunded legislative mandate, some visionaries will see it as an opportunity to more effectively and efficiently leverage their information assets, gain competitive advantage, and contribute positively to our society.

* CGF would like to thank Russel M. Opland for his vast insight and contribution of this article.

CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

About CGF Research Institute (Pty) Ltd

CGF is a Proudly South African company that specialises in conducting desktop research on Governance, Risk and Compliance (GRC) related topics. The company has developed numerous products that cover GRC reports designed to create a high-level awareness and understanding of issues impacting a CEO through to all employees of the organisation.

Through CGF's strategic partners -- supported by our Corporate Patrons *iS Partners, Rifle-shot Performance Holdings and DQS South Africa* -- our capabilities extend to GRC management consulting, executive placements, executive mentoring, company secretariat and the facilitation of Corporate Governance and Risk Awareness workshops. To find out more about CGF, our patrons and our associated services, please access *www.cgf.co.za* or *www.corporate-governance.co.za*

About Russell M. Opland

Russell Opland is your trusted Privacy Advisor. He was formerly an Associate Director in PwC South Africa's Advisory Practice. He has over 10 years of operational and strategic privacy experience as a Chief Privacy and Information Security Officer developing, implementing, and leading privacy programmes with large and complex organisations in the United States. Russell holds a Masters degree in Public Health, and is a Certified Information Privacy Professional (CIPP) and Certified Information Security Manager (CISM) and has served on the boards of several non-profit organisations.

Words: 2,111

Further Media Information:

Terry Booysen (CEO)
CGF Research Institute (Pty) Ltd
Office: (011) 476 82 64 / 1 / 0
Cell: 082-373 2249
Fax: 086 623 1269
Email: tbooysen@cgf.co.za

Further information on Privacy:

Russel M. Opland (Independent Consultant)
Cell: 076-400 2316
E-mail: russopland@gmail.com

PROUDLY SOUTH AFRICAN