



PROCEEDINGS OF THE  
11<sup>th</sup> ANNUAL CONFERENCE  
ON WORLD WIDE WEB APPLICATIONS

2-4 September 2009  
Port Elizabeth  
South Africa

Editor:  
P.A. van Brakel

Publisher:  
Cape Peninsula University of Technology  
PO Box 652  
Cape Town  
8000

Proceedings published at  
<http://www.zaw3.co.za>

ISBN: 978-0-620-45215-1

## TO WHOM IT MAY CONCERN

The full papers were refereed by a double-blind reviewing process according to South Africa's Department of Education (DoE) refereeing standards. Papers were reviewed according to the following criteria:

- Relevancy of the subject to Web applications
- Explanation of the research problem & investigative questions
- Quality of the literature analysis
- Appropriateness of the research method(s)
- Adequacy of the evidence (findings) presented in the paper
- Standardised referencing style.

The following reviewers took part in the process of evaluating the full papers of the 11th Annual Conference on World Wide Web Applications, held from 2 tot 4 September 2009 in Port Elizabeth:

Prof J Brits  
Faculty of Information Sciences (Dean)  
University of Wisconsin  
Milwaukee  
USA

Prof T Carr  
Centre for Higher Education Development  
University of Cape Town  
Cape Town

Prof J Cronjé  
Faculty of Informatics and Design (Dean)  
Cape Peninsula University of Technology  
Cape Town

Mr Craig de Beer  
Web Management Services  
Massey University  
Palmerstone  
New Zealand

Prof M Erasmus  
Management Information Systems  
Erasmus Associates  
Lynnwood  
Pretoria

Dr AM El-Sobky  
Educational Sciences  
RITSEC  
Cairo  
Egypt

Dr MWH Labour  
Laboratory of the Sciences of Communication  
University of Valenciennes and Hainaut Cambrésis  
Valenciennes Cedex  
France

Prof S Mutula  
Department of Information Science  
University of Botswana  
Botswana

Dr David Raitt  
European Space Agency  
The Hague  
The Netherlands

Prof A Singh  
Department of Business Information Systems  
University of KwaZulu-Natal  
Durban

Prof P Weimann  
Economics and Social Sciences  
University of Applied Sciences  
Berlin  
Germany

Further enquiries:

Prof PA van Brakel  
Conference Chair: Annual Conference on WWW Applications  
Cape Peninsula University of Technology  
Cape Town  
+27 21 469 1015 (landline)  
+27 82 966 0789 (mobile)

# The future of information security in the light of the Protection of Personal Information Bill

V Etsebeth  
IT Department  
Edward Nathan Sonnenbergs Attorneys  
Johannesburg, South Africa  
vetsebeth@ens.co.za

## Abstract:

Traditionally, companies conducted business in the physical world where the protection of corporate information/data could effectively be achieved through the implementation of physical security measures. For some time now, however, companies have been conducting business in a digital corporate environment that is faceless, borderless and anonymous. Gone are the days when management had to ask their employees whether or not they would be able to obtain certain information. The problem of a shortage of information is an unpleasant distant memory. The question that now gives management sleepless nights relate to how they should go about protecting sensitive information/data in their possession.

Companies have now come to realise that they have a legal obligation to protect information/data under their control. They know that failure to honour this obligation can lead to unfavourable legal consequences. It is, however, not only companies that are waking up to data protection and privacy challenge. Worldwide, legislatures have also come to recognise the increased importance of data protection and have reacted by developing statutory and regulatory provisions pertaining thereto. The legal position in South Africa is no exception. The new Protection of Personal Information Bill attempts to bring South Africa's data protection practices in line with that of the international community. This Bill, said to be enacted end 2009, early 2010, will undeniably change corporate South Africa's data protection practices. This paper will provide companies with practical guidance on how to become compliant with the Bill. Moreover, it will highlight potential legal pitfalls for companies.

**Keywords:** Information security, data protection, privacy, legal liability.

## 1. Introduction

Personal information has always been a valuable commodity. In the past, however, it was much harder to acquire. Currently, with the advent of the information age and associated technological developments, personal information is easier to steal than ever before.

In the past individuals mainly disclosed their personal information in written form to a selected few. Consequently, when a company needed personal information they first

had to obtain the consent and cooperation of specific individuals before being allowed access to such information. As a result of this, individuals exercised control over who had access to their information, for what purpose the information could be used, and whether or not the information could be transferred to another person/company.

According to Schneier (2008:93) the information age and associated technological developments resulted in three major consequences for individuals:

- (i) “We leave data everywhere we go” - From the ATM that an individual uses to his retail affinity cards, personal emails and even sms messages;
- (ii) “What happens to our data happens to ourselves” - Our data is constantly being ‘touched’ by others; and
- (iii) “Who controls our data controls our lives” - When an individual applies for a home loan his data will determine whether or not it will be granted. When he wishes to travel, his data will determine whether or not he will be granted a visa.

Although the ways in which an individual’s privacy may be infringed have not changed, the manner in which the infringement may occur have. Currently, when for instance the South African Revenue Services (SARS) wishes to investigate an individual’s financial activities they will more than likely search through his personal financial data than obtain a search warrant and search through his home looking for paper-based copies that he may have thrown away or hidden. More alarming is the fact that if a revenue collection agency in another country requests an individual’s personal financial information from SARS, SARS could transfer this information across-borders without the relevant individual ever having consented thereto.

## **2. Traditional Privacy Protection in South Africa**

### **2.1 Introduction**

The right to privacy was first mentioned in South African law in 1898 the case of *De Fourd v Cape Town Council* 1898 (15) SC 399. In one of the leading cases on privacy infringement, *National Media Ltd v Jooste* 1996 (3) SA 262 (A) at 271 the right to privacy was defined as “[T]he right to determine the destiny of private facts and...includes the right to decide when and under what conditions private facts may be made public”.

In terms of South African common law, the concept of privacy is regarded as an independent personality right which is protected in terms of the South African law of delict. The right to privacy as an independent personality right was first confirmed in *O’Keeffe v Angus Printing and Publishing Co Ltd and Another* 1954 (3) SA 244 (K).

Apart from common law protection, the Constitution of South Africa Act 108 of 1996 also recognises the right to privacy as a fundamental right. Section 14 defines the right to privacy as “...everyone has the right to privacy, which includes the right not to have - ... (d) the privacy of their communications infringed”. Section 32 furthermore states that

“(1) [e]veryone has the right of access to – (a) any information held by the state, and; (b) any information that is held by another person and that is required for the exercise or protection of any rights; (2) [n]ational legislation must be enacted to give effect to these rights, and may provide for reasonable measures to alleviate the administrative and financial burden on the state”. It should, however, be borne in mind that section 14 does not afford persons an absolute right to privacy, as all rights in the Constitution may be limited by making use of the general limitation clause contained in section 36. Furthermore, any act, rule or statute that is in conflict with the Constitution will be declared unconstitutional. Neethling et al (2005:31) states that in terms of South African law a two-fold test will be employed when wanting to determine whether or not a person’s constitutional right to privacy has been infringed. Two questions will have to be asked in this regard: (i) did the person have a subjective expectation of privacy? And (ii) was this expectation recognised by society as being reasonable? It is furthermore important to note that fault is not a requirement for an action based on the infringement of the constitutional right to privacy.

## 2.2 Shortcomings in the common law and Constitutional approaches

Regardless of whether a common law or constitutional approach to privacy infringement cases is followed, both approaches contain several material inadequacies. Roos (2008:4) observes that “[t]he traditional delictual principles provide only limited protection for individual’s personal information”. Currently, the common law and the Constitutional privacy protection provisions do not afford individuals the right to:

- (i) actively control who collects, stores, processes, transmits and communicates their personal information;
- (ii) access their personal information held by others;
- (iii) amend their personal information held by others;
- (iv) require their consent prior to collection, storage, processing, or transmission of their personal information;
- (v) be informed of the purpose for which the personal information is collected, stored, processed, transmitted or and communicated;
- (vi) be informed for which time period their personal information will be retained;
- (vii) demand that their personal information be removed from a specific database;
- (viii) prohibit the transfer of their personal information cross-border;
- (ix) insist that companies collecting their personal information have adequate information security measures in place;

Apart from the above mentioned shortcomings, one of the most important reasons South Africa’s current common law and the Constitutional privacy protection landscape is inadequate, is of the fact that South Africa currently does not comply with the EU Data Protection Directive, which is the leading international authority in the domain of

privacy and data protection. This Directive requires countries to implement national legislation that focuses solely on the privacy protection of its citizens. Although it is acknowledged that South Africa is not a member of the EU and therefore does not have to comply with this Directive, international business partners will simply cease dealing with countries that do not follow similar privacy and data protection principles as those set out in the Directive. The USA has already realised this and has taken active steps to ensure that they implement legislation that demands the same level of privacy and data protection of US companies as that of the Directive. In this regard Roos (2008: 433) correctly observes: “[i]t is evident that current South African legislative provisions regarding the protection of personal information are not nearly sufficient when measured against international norms and standards”.

Kang (1998: 1193) correctly observes, that as is the case in America, in South Africa “it is unusual ...to find any comprehensive privacy laws, which legal experts term ‘omnibus laws’ and that enumerate a complete set of rights and responsibilities for those who process personal data”. Privacy legislation is generally sector specific, levelled at very narrow categories of data. The focus of these statutes is generally limited to financial data and credit reports, leaving the private sector relatively unregulated. Pursuant to the above it is hardly surprising that serious inadequacies currently exist in the South African privacy landscape.

If South Africa wishes to remain a serious player in the international arena it has no choice but to follow suit. Currently, the mantra “adapt or die” is very apt for South Africa’s privacy and data protection situation.

### **3. Challenges facing online privacy protection**

As have been stated above, individuals have lost complete control over their personal information. In the past, personal information were only provided to a selected few who had to provide guarantees that such information would remain under lock and key to ensure that it did not fall into the wrong hands. At present, however, this luxury no longer exists. Solvo (2004:22) correctly observes that “cyberspace is the new frontier for gathering personal information and its power has only began to be exploited”. Apart from the fact that companies indiscriminately share customer information/data with one another with little or no consideration being given to the privacy of such information, individuals no longer have any control over where their information resides, who has access to it, who it is shared with and for what purposes it is used. Even more alarming is the fact that even if an individual’s personal information is misused or disclosed to an unauthorised party, the individual will seldom have any knowledge of this. Alternatively, even if the individual becomes aware of the fact that he has fallen victim to identity theft the legal avenues at his disposal are costly and time consuming.

Web-based companies have furthermore come to realise the value of information collecting tools. These companies mostly make use of two methods to collect information, namely (i) the website directly request data from users; and (ii) the website secretly tracks a user’s online movements. The latter method is at present the most popular method of information collection.

Pursuant to the above, it is evident that from the moment a user connects to the internet, until the time he disconnects, users create digital footprints which companies, and more alarmingly, adversaries can view, trace and use against a specific user (Solvo 2004:25). Legislatures and governments alike have come to realise the inherent risks involved in allowing companies to use personal information indiscriminately. Consequently, a need for comprehensive data protection laws was recognised. These laws will, however, have to meet the following requirements:

- (i) they should protect all personal information about individuals;
- (ii) they should limit another's ability to buy and sell personal information without the relevant individual's consent;
- (iii) they should allow individuals to view information held by others about themselves;
- (iv) they should provide individuals with the opportunity to amend and correct any inaccuracies;
- (v) they should enforce data deletion and retention practices;
- (vi) they should limit data collection; and
- (vii) they should have effective enforcing mechanisms in place (Schneier 2008:62).

#### **4. Key developments in South Africa's privacy legislation**

##### **4.1 Introduction**

In response to the increased attention privacy and data protection received internationally, the South African Legislature has commenced addressing the issue, be it very briefly, in several statutes.

- (i) the Electronic Communications and Transactions Act;
- (ii) the Promotion to Access to Information Act; and
- (iii) the Protection of Personal Information Bill.

##### **4.2 The Protection of Personal Information Bill**

The recent Protection of Personal Information Bill represents a new development in the South African law of privacy.

This Bill is based on eight core principles, namely:

- (i) information can only be collected or stored if it is necessary for explicitly defined purpose and does not intrude upon the privacy of the data subject to an unreasonable extent. This principle implies that a data controller may only collect and store personal information: (a) to the extent necessary to achieve an explicitly defined purpose; and (b) the storage does not intrude on privacy of the data subject to an unreasonable extent. Consequently, if a data controller wishes to use personal information for any other unspecified purposes, he will only be able to do so once he has obtained additional consent for this from the data subject. Furthermore, the purpose for which the personal information is collected must be specified and determined at the time of collection and disclosed to the data subject. It goes without saying that the purpose of collection must be lawful;

- (ii) information must be collected directly from and with the consent of the data subject. This principle implies that the specific consent of the data subject personally is required and that service providers must provide warranties that information was obtained with the personal consent of the data subject. Consent may be obtained in one of two ways: (a) opt-in option, where the data subject is deemed not to consent unless he specifically grants consent by for instance, checking a box; and (b) opt-out option, where the data subject is deemed to consent unless he specifically discontinues consent. In this instance there will already be a tick in the box. The Bill is not prescriptive in this regard, however, the safest option would be the opt-in approach;
- (iii) data subjects must be informed of the purpose of the collection and the intended recipients of the information. This principle implies that (i) the purpose for which the data is collected must be disclosed; (ii) disclose to the data subject who the intended recipient of the information is; and (iii) logs and other records which provides evidence of disclosures to data subjects must be governed effectively;
- (iv) information must not be retained for longer than is necessary to achieve the purpose for which it was collected. This principle implies that (i) record management and email archiving must effectively be governed; and (ii) service providers who come into contact with the information must provide warranties pertaining to the return and destruction of information when requested. Neither the Bill nor the ECTA specifies the period for which information must be retained. Notable is the Bill's provisions relating to data destruction. The Bill prescribes that data must be destroyed at the end of the period or when it is no longer in use. This Bill is the first piece of legislation in South Africa to ever focus attention on the destruction of electronic data. Moreover, the Bill makes it clear that the data controller bears the cost of retention and destruction of the data. Companies should, however, bear in mind that data and information deletion does not equate with destruction;
- (v) information must not be distributed in a way incompatible with the purpose for which it was collected. This principle implies that (a) the data subject has consent to the onward transfer of his personal information; and (b) the data controller has gained assurance that the recipient data controller has adequate information security safeguards in place to protect the privacy of the information;
- (vi) reasonable steps must be taken to ensure that the information processed is accurate, up-to-date and complete. In terms of this principle the data controller bears responsibility for verifying the accuracy of information received. Consequently, the data controller will have to implement information security measures to ensure that a user does not masquerade as another.
- (vii) appropriate technical and organisational measures have to be taken to safeguard the data subject against the risk of loss, damage, destruction of, or unauthorised access to, personal information. This principle implies the identification and mitigation of risks and the implementation of: IT security

controls and measures; information security controls and measures; policies; agreements and insurance; and

- (viii) data subjects are allowed a right of access to their personal information and a right to demand correction if such information is inaccurate. This principle demands that data subjects must be: (a) able to access and amend their personal information; (b) entitled to demand that their personal information is removed from a system; and (c) entitled to stipulate that their personal information may not be transferred to third parties.

## **5. Legal obstacles in online privacy infringement cases**

### **5.1 How will the nature of the claim be determined?**

One of the main difficulties that will be encountered with online privacy infringement cases relates to the uncertainty surrounding the nature of cyberspace. Generally when judging privacy claims courts rely on the nature of the claim to determine whether or not it is worthy of protection (*Griswold v Connecticut* (381) US 479 1965).

#### **5.1.1 The nature of the claim**

When courts wish to determine the nature of a claim based on privacy infringement, they first have to answer the problematic question of whether cyberspace is in the public or private domain.

American courts generally accept that “anything capable of being viewed from a ‘public place’ does not fall within the privacy torts’ protective umbrella”. When asked, most people are of the opinion that the internet is public, because almost anyone can access it at any time from any place in the world. Uncertainty, however, still remains with courts regarding the public and/or private nature of cyberspace. A starting point to answering this question is the development of an acceptable definition for cyberspace. No universally acceptable definition has yet been formulated by the courts. Some legal theorist suggests that cyberspace should be viewed analogue to physical space, while others reject the limits of traditional physicality.

From a survey of South African case law it is evident that although the courts have used the term ‘cyberspace’ in several cases, they have never attempted to define it. American courts have similarly been unsuccessful in their efforts to develop an acceptable legal definition for cyberspace. Abril (2008:30) correctly observes that “[w]hile several cases have struggled with the concept of location of cyberspace, there is no definitive judicial construction of space and place in cyberspace”. As a result of the aforementioned it follows that courts have also failed to agree on whether the internet is public or private in nature. When considering the characteristics of the internet, namely that it is faceless, borderless and anonymous place it is not far fetched to argue that the internet is public in nature. The author submits that information placed voluntarily on the internet will fall within the public domain unless access to the information is restricted, (for instance through password protection). If access to certain information such as

information on facebook is password protected, a strong argument can be made that the author never intended that the information to be available to the general public but only wanted it to be viewed by a selected view.

### 5.1.2 The value of information

The second problematic question courts must address relates to the value of personal information, and more specifically, whether the information under discussion is worthy of protection.

Solvo (2008: 87) submits that the value of personal information “is determined by how much it takes for a person to relinquish it”. He proceeds to observe that currently individuals effortlessly provide information when applying for credit cards, retail store cards or access to specific websites. This may lead to the conclusion that the value of such information is relatively low to the specific individuals. However, it must be borne in mind that individuals provide certain information in specific contexts to, for instance financial institutions or health care insurers. At first sight these fragmented pieces of information will appear to be irrelevant and useless. Solvo (2008: 87) However, when all these pieces of information pertaining to a specific individual are combined the risk of privacy infringement increases exponentially. Professor Julie Cohen observes in this regard: “[i]t is the totality of information about a person and how it is used that poses the greatest threat to privacy”. (Solvo, 2008: 87)

When taking into account the infinite number of potential future uses of personal information it is understandable that courts will encounter great difficulties in determining the true value of the personal information that has been compromised. Solvo 2008:87 correctly observes that the value of personal information does not relate to the intimacy of the information but rather in an individual’s ability to “prevent others from gaining power and control over an individual”.

## 6. Conclusion

Solvo (2004:223) observes that technology should ideally empower users by giving them more control and making users more secure. At present, however, technology has had exactly the converse effect. Individuals have lost complete control over their personal information and most individuals are very sceptical when it comes to security and technology.

Solvo (2004:223) observes that although one cannot claim that the law has failed in the domain of privacy and data protection, one is also unable to claim that the law has succeeded in this domain. There are those that argue that individuals should accept that they have lost complete control over their information and that it is an impossible to regain control. McNealy is a proponent of this view. He observes in this regard: “[y]ou already have zero privacy. Get over it” (Solvo, 2004:224). Etziani concurs “[t]o be realistic...the probability of returning the genie to the bottle is nil” (Solvo, 2004:224).

Currently, the misconception prevails amongst internet users that technology erodes privacy. Solvo 2004:224 however, disagrees with this cynical outlook. He argues that most privacy and data protection problems do not arise because of technology, but rather because of law, and more specifically the inadequacy thereof. He goes on to observe that “[t]he law actively contributes to the creation of our dossiers by compelling people to give up personal data, placing in the public records, and then allowing it to be amassed by database computers”(Solvo 2004:227). It is submitted that one of the biggest mistakes legislatures world-wide make is to draft legislation reactive to new technology (Solvo 2004:224). Good laws should be created independent of technology. (Solvo 2004:225) observes in this regard:

“[m]any privacy problems are the product of legal decisions that have been made over the past century as we have shaped our information economy. Once we understand the full extent of the legal construction of privacy, we will realize privacy is not passively slipping away but is actively being eliminated by the way we are constructing the information economy through law”.

The new Protection of Personal Information Bill attempts to bring South Africa’s data protection practices in line with that of the international community. One of the main difficulties experienced in this regard relates to finding a satisfactory balance between the obligation to protect an individual’s right to privacy and a company’s need to gather and process personal information in order to function effectively. The legislature should furthermore realise that introducing corporate South Africa to data protection legislation involves more than a mere ‘cut and paste’ exercise. Privacy legislation will have to be flexible enough to adapt to the unique challenges South Africa is faced with. Moreover, it is pivotal that the legislator realises that South African companies do not have the same monetary and human resources at their disposal as their international counterparts. A very real danger exists that the data protection legislation promulgated by Government can not be implemented due to a lack of resources on the part of corporate South Africa.

Solvo (2004:228) concludes “[t]he law can protect privacy. This does not require that the law become involved in areas in which it currently has been absent – the law is already involved. The choices we make in shaping the law are of critical importance”.

## 6. List of references

Abril, S. 2007. Recasting privacy torts in a spaceless world. *Harvard Journal of Law and Technology*, Vol. 21.

Kang, J. 1998. Information Privacy in Cyberspace Transactions” 50 *Stanford Law Review* 1193.

Neethling, Potgieter & Visser 2005 *Law of Personality*. Durban: Butterworths.

Roos, A. 2008. Data protection: explaining the international backdrop and evaluating the current South African position 4 PER 92.

Rosen, A. 1997. *Looking into intranets and the Internet: advice for managers*. New York: American Management Association.

Schneier, B. 2008 *Schneier on Security*. John Wiley & Sons.

Solvo, D. 2004 *The Digital Person*. New York: New York University Press Publication.

**Case law:**

*De Fourd v Cape Town Council* 1898 (15) SC 399

*Griswold v Connecticut* (381) US 479 1965

*National Media Ltd v Jooste* 1996 (3) SA 262 (A)

*O'Keeffe v Angus Printing and Publishing Co Ltd and Another* 1954 (3) SA 244 (K)