



PROCEEDINGS OF THE
11th 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)

Privacy policy statements and their compliance to the ECT Act: the case of South African banks

S.K. Kabanda

Department of Information Systems
University of Cape Town
Cape Town, South Africa
Salah.kabanda@uct.ac.za

I. Brown

Department of Information Systems
University of Cape Town
Cape Town, South Africa
Irwin.Brown@uct.ac.za

V. Nyamakura

Department of Information Systems
University of Cape Town
Cape Town, South Africa

J. Keshav

Department of Information Systems
University of Cape Town
Cape Town, South Africa

Abstract

With the increased need for fast and yet cheaper ways of communication, companies are now increasingly adopting Internet related technologies such as Electronic Commerce (E-Commerce) and Internet banking. Although these technologies have improved customer services, they have also brought in privacy and security issues concerning customer protection over the internet. This is more so in the banking sector which deals specifically with customers' private information. Although there have been various studies on online security and privacy regulations, few have concentrated on the privacy policy statements of South African banks and their compliance with the rules of the Electronic Communications and Transactions Act (ECT Act) and the impact that these rules and the compliance to the ECT Act, have on the consumers. This empirical report is an attempt to examine this phenomenon. The study used a content analysis, followed up by interviewee sessions. The results showed that South African banks do not comply with all the provisions of the ECT Act and there were inconsistencies across banks in terms of the presence, accessibility and readability of the privacy policy statements.

Keywords: Privacy, business confidence, trust, privacy policy statements, ECT Act

1. Introduction

As the internet and technology expands, companies have had to enhance their capacities to collect and analyse data about customers who are increasingly using the internet for transaction purposes. There are various advantages that have risen from

this expansion, for example, the internet has increased the speed and convenience of data collection. However, there are also many problems associated with the internet, such as security and privacy. The banking industry is no exception as it deals specifically with the private information of customers. Banks have adopted these new technologies such as internet banking which has given rise to various privacy and security issues concerning customer protection over the internet (Baumer & Earp, 2003). In South Africa alone, it is estimated that there are about 3 million internet users that engage with banking internet transactions on a daily basis (Goldstruck, 2002). Unfortunately most of these users often provide their personal information to the websites without understanding the reason as to why their information has to be collected or shared (Goldstruck, 2002). Others are now becoming aware of websites monitoring their actions and they are becoming doubtful about the protection of their private information (Graeff & Harmon, 2002).

Protection of customer information is an important element of an organization as it is vital to the establishment of business confidence between E-Commerce websites and customers (Iyer, Palvia, Salam & Singh, 2005). Business confidence develops where the participants in a transaction feel secured and assured that only authorized users have access to information; that the quality of the information being accessed is complete, uncorrupted and easily accessible (McConnell, 1994). However, online customers are reported to display low business confidence with E-Commerce websites because of hackers and the ongoing debate about privacy issues (Culnan and Armstrong, 1999; Hoffman et al., 1999). This is more so for the Internet banking sector that require sensitive information such as financial information and credit card numbers (Ackerman, Cranor & Reagle, 1999; Cazier, Shao & St. Louise, 2003; Baumer & Earp, 2003; Arcand, Ales-Dufor, Nantel & Vincent, 2007).

In South African, the Internet banking sector started in 1996 and has since then opened new opportunities for its consumers to have control over their finances (Singh, 2004; Green & Van Belle, 2003). To regulate the electronic environment and protect consumers, the South African government developed the Electronic Communications and Transactions Act (ECT Act) in August 2002. However, Van Belle and Joubert (2004) note that most internet banking websites do not fully understand this act. It is against this observation that we ask: do South African internet banking websites comply with the ECT act - an act they do not fully understand? And what are the impacts thereof on consumers? The study focuses on compliance of the banks to the ECT Act because compliance acts as a measure of safeguarding the consumer against privacy issues.

The rest of this paper is structured as follows: The next section provides a background to Electronic Commerce and privacy related issues. The section also introduces the laws in South African for regulating the Electronic environment. Section 3 provides the research methodology. Section 4 discusses the findings and Section 5 concludes the study.

2. Related work

2.1 Privacy as a challenge in electronic commerce

As electronic commerce become more established and dependable, attention is turning towards identifying critical success factors of a website (Corritore, Kracher and Wiedenbeck, 2003). Among the many critical success factors, the issue of trust takes

the forefront and is currently the third of the top ten barriers and inhibitors of e-commerce and any successful business strategic alliances (Corbitt et al, 2003). Trust is key because of the risky and uncertainties posed by the electronic commerce environment. These risky and uncertainty situations include security and privacy concerns. Privacy concerns are increasingly becoming a challenge in the Electronic environment and have received significant attention to-date.

Gutwin & Levy (2005) defined privacy as an issue of control over the inflow and outflow of information. It is a moral claim and the right of an individual to determine what happens to his or her personal information that is gathered by another party. Issues of privacy concerns have been so widespread in E-Commerce so much so that in the early 1960's, many countries started developing privacy laws and regulations to safeguard the customer's information (Laudon, 1996). In South Africa, privacy and security regulations have been investigated and the government has laid down various laws regulating the Electronic Environment (Van der Merwe, 2003; Van Belle et al, 2004; Singh, 2004; Van Belle and Joubert, 2004; Kyobe, 2005). These laws are discussed in the next section.

2.2 South African electronic environment regulators

The Electronic Communications and Transactions Act (ECT) consist of fourteen chapters and ninety-five sections. Of interest to this study is the privacy related concerns of Chapter 8, Section 51 which deals with the protection of a customer's personal information when conducting electronic transactions. The section consists of nine principles which address guidelines on information privacy control as depicted in Table 1. According to the Act, "a data controller must subscribe to all the principles outlined in section 51". For example banks, are required to inform the consumer about the purpose of information collection; the content and nature of the personal information that is being collected; and a guarantee to the consumer that the collected information will not be disclosed to a third party without consumer consent.

Table 1: ECT Act nine Principles of Section 51, Chapter 8.

Principle	Statement
1	A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
2	A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
3	The data controller must disclose in writing to the data subject specific purpose for which any personal information is being requested, collected, collated, processed, or stored
4	The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject unless he or she is permitted or required to do so by law.
5	The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and specific purpose for which the personal information was collected.
6	A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorized to do so in writing by the data subject.

7	The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed, the date on which and the purpose for which it was disclosed
8	The data controller must delete or destroy all personal information which has become obsolete.
9	A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, provided that the profiles or statistical data cannot be linked to any specific data subject by a third party

The Act together with the Protection of Personal Information (PPI) Act aims at safeguarding a person's personal information when processed by public and private bodies. The PPI Act applies to the fully or partly automated processing of personal information, and the non-automated processing of personal information entered in a record or intended to be entered therein. The personal information may only be processed given the purpose(s) for which it is collected or subsequently processed, it is adequate, relevant, and not excessive; and data subject has given consent for the processing and is aware as to why the data was collected and is being processed for. Together, the two acts including the rights in the Bill of Rights in Chapter 2 of the Constitution, particularly the right to access to information, need to be adhered to and conveyed to the consumer. The acts are usually conveyed to the consumer through the websites' privacy policy statement (Van Belle & Joubert, 2004).

A privacy policy statement is a strategic tool that not only tackle privacy issues by stating how the site will use personal identifiable information (PII) that is collected from fields and forms in web-based transactions (Gutwin & Levy, 2005) but it also act as a tool for increasing customer trust (Arcand et al., 2007; Criswell, Crossland, Meinert & Peterson, 2007). In this manner, the privacy policies statement helps to inform customers of privacy practices and help aid them in making decisions. A study conducted by Furnell & Karwani (1999) indicated that 85% of internet users expected to find a privacy policy statement when visiting e-commerce websites and 66% felt more confident and secure with websites that had a mere presence of a privacy statement

3. Research methodology

The purpose of the study is two fold: firstly to investigate compliance of the banks to the ECT act; and secondly to investigate the impacts of (non)compliance on consumers. The investigation adopted a content analysis technique - an observational research method used to systematically evaluate the symbolic content of all forms of recorded communications that can analysed as texts. Content analysis has been used before in researches about websites and privacy policies (Cappel & Huang, 2007). In this study, the websites of South African banks were analysed using content analysis, to identify a privacy policy presence that meets the ECT Act. The observation employed Hooper and Johnston (2008) instrument which followed the ECT act's nine principles to determine compliance. In addition, the instrument investigated how easy the privacy statement was to access, read and understand. There were 36 registered banks in South Africa and of these 14 banks were South African controlled (South African Registered banks, 2008). Of the 14 banks, Regal Treasury Private Limited was not included as it is under curatorship and the website was no longer available. We then conducted interview sessions with 10 internet users from the four major banks. The internet users were all postgraduate students at the University of Cape Town. The purpose of the interview was three fold. Firstly to understand user's interpretation of the "privacy policy statement". Secondly the interview rationale was to investigate the impact of a privacy policy statement to them. Thirdly, to assess the "understandability" aspect of the privacy policy statement. After the interview content

analysis was further employed to identify common themes in the interview. To assess readability of the privacy policy statements, Flesch Reading Ease Score (FRES) was used (Jensen & Potts, 2004).

4. Results and discussion

4.1 Presence of Privacy Policy Statement and Compliance to the ECT Act

Results indicate that 69% of South African banks posted a privacy statement on their website with some stating the importance of customers reading their privacy policy statement prior registration as internet bank users. These banks are either trying to meet the law or do understand that a privacy policy statement aids decision making for customers, hence its importance. The rest of the banks however did not have a privacy policy statement at all nor any other form that conveys privacy related issues to consumers. During the interview process, interviewees were asked of their views on the absence and presence of a privacy policy statement. Respondents were also asked as to whether they knew what a privacy policy statement involved. All respondents indicated their awareness of what a privacy statement was and how it was concerned with privacy issues, regulations and protection of personal information, but they were unsure and some unaware of its existence on the bank's website. However, most thought it was important for organizations to put a privacy statement on their website because, according to Interviewee 5:

“it would show what the banks were going to use the information for and the restrictions that are placed on the banks” and “it would show the implications of using the internet with regards to disclosure of personal information” as well as “show us how the bank would not only protect the customer but themselves as well” [Interviewee 5].

Most interviewees believed that through a privacy policy statement, they would be able to assess the banks trustworthy

“I think most consumers will believe that the bank is doing the right thing. I think it's very important especially information that you happen to be disclosing with your bank. I mean they got some pretty sensitive information there and I think it's a vital component in ensuring your security apart from anything else. Having information floating around, that sort of type of information about you and if it gets into the wrong hands I think that can cause a security problem in effect [Interviewee 10]

However, there were some interviewees who did not seem to agree to the importance of the privacy policy statement:

“I don't think it's important because I'm pretty sure companies make a privacy statement without actually adhering to it because a lot of the times, we don't know what happens behind closed doors or we don't get to see what happens. So in that aspect, I don't think it's important.” [Interviewee 6]

There was a general view amongst the respondents that the mere existence of the privacy statement made them perceive that the website had a privacy statement that complied with the ECT Act. Thus as noted by Furnell & Karwani (1999), the mere existence of a privacy statement has a positive effect on customer perception of the bank.

Of the 69% of banks that had a privacy policy statement, none of them adhered to all the principles of the ECT Act. For example, it was noted that in order to get consent from customers, most banks inserted a clause that stated that by reading the privacy statement, the customers agree to share their personal information with third parties. This is in contrary to what principle 1 of the ECT Act says “A data controller must have the express written permission of

the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law” (see Table 1). The clause inserted by the banks does not equal “express written permission of the data subject” because the users has not provided printed consent.

Principle 4 on the other hand prevents the banks from using a customer’s information for any purposes other than those stated in the privacy statement. Unfortunately from the analysis, only 15% of the banks gave the customers the option to give consent for the use of their personal information for other purposes. 69% of the banks did not give customers the option of giving the banks consent and the remaining 16% of the banks partially fulfilled this principle. Principle seven states that the data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed, the date on which and the purpose for which it was disclosed. Even though most of the banks stated that they would disclose information to third parties, 92% of the banks did not state this principle in their privacy statements and as of those who did, few of them mentioned who the third party was (third parties included affiliate parties, subsidiaries, shareholders and business partners). With regard to banks disclosing information to third parties without the consent of the customer, most interviewees were not pleased to the extent of some considering changing banks. Interviewee 4 stated:

“That is very misleading and it is very unethical from them to do so. It will most probably destroy my confidence in the bank.” [Interviewee 4]

“... I would feel like I’m not protected enough. I would sort of feel not, really violated, if nothing has happened yet but I would feel that there is room for violation. I would probably have to change my bank” [Interviewee 5].

Some of banks did not specify the reasons for which the personal information is being requested although required to do so by law. With regard to this, Interviewee 8 stated:

“I wouldn’t trust them because I would want to know what’s happening with my information, where is it being taken to and for what purposes. Because if its mine, it’s my private information and I have the right to know. So I wouldn’t trust a bank that would give out the information without my consent or with my consent but not disclosing the purpose for giving out the information.” [Interviewee 8]

4.2 Readability and understanding of privacy statement

The content analysis results showed that all the privacy statements were complex, difficult and lengthy to read. They contain difficult words such as “Cookies” and “Encryption” which are difficult to understand if one is not in the Information Technology discipline. However, some banks did define these complex terms. Table 2 shows the Flesch reading ease score for the South African banks that had privacy statements. All the banks had a Flesch grade level above 12. The implication is that for the privacy statement to be understood, the user must have had at least 12 years of formal education. The length of the privacy statements was also deterring them from reading it. For example, Interviewee 9 responded that:

“...I assume it’s important but because it is too long, I have never read it. There is someone looking out for you so I don’t have to read it because someone makes sure it is up to standard.” [Interviewee 9]

Table 2: Flesch Reading Ease Score for South African Banks

Bank	Words	Flesch Score	Flesch Grade Level	Readability Level
------	-------	--------------	--------------------	-------------------

A	787	24.5	15.6	Very Difficult
B	940	40.5	13.6	Difficult
D	241	24.2	13.8	Very Difficult
E	277	38.2	14.0	Difficult
G	1143	30.7	16.2	Difficult
H	244	35.0	14.4	Difficult
I	938	33.2	13.9	Difficult
J	435	44.2	12.8	Difficult
L	498	23.3	17.9	Very Difficult

Apart from the readability, none of the banks posted their privacy statements in the South African official languages. This makes it more difficult for local users who are not familiar with the English language. The responses from the interviews reflected the need for accommodating local languages, especially given the fact that few of the people are able to attend tertiary institutions.

4.3 Accessibility/location of privacy statement

Accessibility of the privacy policy statements was assessed in terms of how easy it was to access the privacy policy. This was assessed in terms of where the privacy policy statements were positioned or located on the bank's website. Figure 4 below indicates how accessible the privacy policy statements were. Only 23% of the privacy policy statements were displayed on the bank's home page and thus easier to access. However 77% of them were difficult to find as they were posted on the terms and conditions, disclaimer or legal requirements

In addition, most privacy statements are located at the bottom of a web page and usually accessed via a link (for example, by clicking Terms and Conditions). Although the respondents agreed that this location is suitable for consistency sake as supported by Jensen & Potts (2004), they also felt that by it being at the bottom

"... the impression is that the privacy statement is not that important [Interviewee 9]."

4.4 Impact of content of privacy statement on customer perceptions

Most interviewees felt that the privacy policy content would affect their perception of the bank, especially if the content was inadequate or lacking in terms of non-compliance to the ECT Act:

"Knowing it (privacy statement) and knowing exactly what should be in it could change the way I perceive a bank." [Interviewee 7]

"If they were very clear and specific, then I would trust them more. Whereas if they covered themselves by being vague and things then I would probably wonder why they are being vague and probably lose trust". [Interviewee 6]

Interviewees felt that privacy policy content clarity is important otherwise statements can be misinterpreted. However, not all respondents agreed about the importance of the contents. They stated that perceptions of the banks come from advertising, customer service and not from

the privacy statement content. However, some of the interviewees were unsure stating that even though the content of the privacy statement affected their perceptions of the bank, these perceptions were also dependant on certain factors. Interviewee 5 considered factors such as the type of person and the transaction done over the internet to affect how she perceives the bank.

“It does depend on the person you are and what type of transactions you will be doing on the actual internet. If you would be doing transactions like transferring money and all that, I think that is important but if you are just checking your balance, and you are not transferring money then maybe it’s not as important”. [Interviewee 5]

5 Conclusion

The need to secure and protect consumer’s private information has led to the use of Privacy policy statements that state the ways that a site will use personal identifiable information online. To date, many internet related organizations such as banks carry a privacy policy statement which is used as a strategic tool for increasing customer trust and building customer confidence of using the bank. However, the Privacy policy statement need to meet ECT act conditions set down to govern internet related transactions.

This study found that most banks have a privacy policy statement posted on their websites but the statements are not easily accessible and written in English - a language that is foreign to the majority of South Africans. The readability of the privacy statements pose another problem because of the complex terms used and their length. However, users indicated the importance of every bank having a privacy policy statement and the importance of the policy meeting their needs and the ECT Act requirements. Users believe that if the policy meets these requirements, they are able to trust the banks more and ultimately build business confidence with them. The study found that there was a negative impact on business confidence by banks not adhering to the provisions of the ECT Act. When a customer loses confidence in his or her bank, the entire image that the customer has of the bank is affected negatively. This could increase customer doubt and he or she could become sceptical about every facet of that specific bank. Furthermore, a lack of business confidence could also result in a customer changing banking services, in search for assurance and a higher level of business confidence with another bank. The study recommends that:

- All South African banks that provide internet banking services should have a privacy policy statement that is easily available to the public.
- Banks should also consider the alternative of making the privacy policy statement available in other South African official languages as the respondents demonstrated that it would be of benefit for customers who feel more comfortable with their local language.
- There is a need for a regulatory body that reviews the privacy policy statements of banks that use internet banking.

The study was constrained by the few number of internet users interviewed as this would not reflect the general view of all users. Future research needs to investigate the reasons as to why banks do not comply with all ECT Act requirements. There is scope for more research into technologies that would help enhance privacy protection in the South Africa market. In this report, P3P technologies were identified as one of those technologies. However there are other technologies that exist, such as third party certification and privacy seals. Further research into these technologies will aid South African banks and assist in increasing customer trust and level of business confidence in the banks.

6. Reference

Ackerman, M. S., Cranor, L. F., and Joseph, R. 1999. Privacy in E-Commerce: Examining User Proceedings of the 11th Annual Conference on World Wide Web Applications, Port Elizabeth, 2-4 September 2009 (<http://www.zaw3.co.za>)

- Scenarios and Privacy Preferences. *Proceedings of the 1st ACM conference on Electronic commerce* (pp. 1-8). Denver, Colorado, United States : ACM.
- Arcand, M., Arle-Dufour, M., Nantel, J., and Vincent, A. 2007. The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review* , 31 (5), 661-681.
- Baumer, D., and Earp, J.B. 2003. Innovative Web Use To Learn About Customer Behaviour and Online Privacy. *Communications of the ACM* , Vol.46, No.4, 81-83.
- Cazier, J. A., Shao, B. B., and St Loieuse, R. D. 2003. Addressing E-business privacy concerns: The role of trust and value compatibility. *ACM symposium on Applied computing* (pp. 617-622). Melbourne, Florida : ACM.
- Corbitt, B. J., Thanasankit, T., and Yi, H. 2002. Trust and E-commerce: A study of customer perceptions. *Electronic Commerce Research and Applications* , 2, 203-215.
- Corritorea C. L., Krachera B., and Wiedenbeck S.. 2003. On-line trust: concepts, evolving themes, a model *Int. J. Human-Computer Studies* 58 (2003) 737–758
- Criswell, J., Crossland, M., Meinart, D., and Peterson, D. 2007. Customer trust: privacy policies and third-party seals. *Journal of Small Business and Enterprise Development* , 14 (4), 654-699.
- Furnell, S., and Karweni, T. 1999. Security Implications of Electronic Commerce: a survey of customers and businesses. Internet Research: *Electronic Networking Applications and Policy* , 9 (5), 372-382.
- Goldstruck, A. (2002). Internet Access in South Africa. [Online] <http://www.theworx.biz/access02.html> (accessed 8 April 2008).
- Graeff, T. R., and Harmon, S. 2002. Collecting and using personal data: Customers awareness and concern. *Journal of Customer Marketing* , 19 (4), 302-318.
- Green, S. and Van Belle, J.P. 2003. Customer Expectations of Internet Banking in South Africa. *Proceedings of the Third International Conference on Electronic Business (ICEB 2003)*. Singapore.
- Gutwin, C., and Levy, S. E. 2005. Improving Understanding of Website Privacy Policies with Fine Grained Policy Anchors. *International World Wide Web Conference* (pp. 480-488). Chiba: ACM.
- Hooper ACS and Johnston KA. 2008. Establishing Business integrity through website statements an exploration of South African banking websites, *Proceedings of the 10th Annual Conference on World Wide Web Applications, www2008*, University of Cape Town . 3-5 September 2008, Cape Town, South Africa [978-0-620-42642-8]
- Iyer, L., Palvia, P., Salam, A., and Singh, R. 2005. Trust in E-commerce. *Communications of the ACM* , 48 (2), 73-77.
- Jensen, C., and Potts, C. 2004. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. *SIGCHI conference on Human factors in computing systems* , 6, pp. 471-478. Vienna, Austria.
- Kyobe, M. 2005. Addressing E-crime & Computer Security Issues in Homes & Small Organizations in South Africa. *European Management and Technology conference on the integration of Management and Technology*, (pp. 1-13). Rome, Italy.
- Laudon, K.C. 1996. Markets and Privacy. *Communications of the ACM* , 39 (9), 92-102.
- McConnell, J. (1994). National Training Standard for Information System Security. <http://www.nstissc.gov/Assets/pdf/4011.pdf>. (accessed 21 January, 2009)
- Singh, A. M. 2004. Trends in SouthAfrican Internet Banking. *Aslib Proceedings: New Information Perspectives* , 56 (3), 187-196.
- Van Belle, J.P. & Joubert, J. 2004. Compliance of South African E-commerce Websites with

Legislation to Protect Customer Rights. *Proceedings of the 2004 International Business Information Management Conference (IBIM '04)*. Amman Jordan.

Van Belle, J.P., Haig, A., Mitchell, C. & Watson, M. 2004a. An Investigation into Customer Data Privacy Protection By Top South African E Commerce Sites. *Proceedings of the Southern Africa Institute of Management Scientists Conference (SAIMS04)*. Cape Town.

Van Belle, J.P., Haig, A., Mitchell, C. & Watson, M. 2004b. Data Privacy and Customer Protection in South African E-Commerce. *Proceedings of the Annual Information Technology Congress (CATI04)*. So Paulo.

Van der Merwe, J. 2003. To what extent do the websites of SA e-commerce companies comply with the provisions of the ECT Act in terms of protection of Consumer rights. Cape Town

Acknowledgements

This material is based upon work supported financially by the National Research Foundation. Any opinion, findings and conclusions or recommendations expressed in this material are those of the authors and therefore the NRF does not accept any liability in regard thereto.