South African banks and their online privacy policy statements: A content analysis

Authors:
Salah K. Kabanda[1]
Irwin Brown[1]
V. Nyamakura[1]
J. Keshav[1]

Affiliations:
[1]Department of Information Systems, University of Cape Town, Cape Town, South Africa

Correspondence to:
Salah Kabanda

email:
salah.kabanda@uct.ac.za

Postal address:
Department of Information Systems, University of Cape Town, Private Bag X3, Rondebosch 7701, South Africa

Keywords:
business confidence; ECT Act; privacy policy statements; trust

Dates:
Received: 13 Nov. 2009
Accepted: 03 July 2010
Published: 30 Sept. 2010

How to cite this article:
Kabanda, S.K., Brown, I., Nyamakura, V. & Keshav, J., 2010, 'South African banks and their online privacy policy statements: A content analysis', *SA Journal of Information Management* 12(1), Art. #418, 7 pages. DOI: 10.4102/sajim.v12i1.418

This article is available at:
http://www.sajim.co.za

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

ABSTRACT

In Internet banking and Internet-related transactions, security and privacy are of great concern. To alleviate these concerns, the South African government has promulgated the Electronic Communications and Transactions (ECT) Act No. 25 of 2002. The Act regulates all electronic communication transactions in South Africa. Business organisations implement the Act by, for example, posting a privacy policy statement on their websites, which, in accordance with the requirements of the ECT Act, states how the organisation will use any personal identifiable information provided by the client. This study investigates whether South African banks that subscribe to the ECT Act comply with the principles relating to the protection of a consumer's personal information. The study employed the research methods of content analysis and interviews. The findings indicate that some banks only complied with a few of the ECT Act principles, which, according to the interview respondents, undermines the levels of trust which are in play between their banks and themselves. The respondents themselves were not fully aware of all the ECT Act requirements. This lack of awareness results in consumers failing to assess the comprehensiveness of their bank's policy statements and to what extent such banks comply with the ECT Act.

INTRODUCTION

The growth of the Internet is changing the way in which corporations conduct business with consumers (Liu & Arnett 2000). The use of the web has enabled mass customisation; improved marketing and communication; innovation, and development of non-core businesses (Cheng, Lam & Yeung 2006; Jayawardhena & Foley 2000). In the banking sector, customers can now perform common banking transactions, such as paying bills, transferring funds, printing statements, and enquiring about account balances online (Arcand *et al.* 2007; Cazier, Shao & St. Louise 2003). Although a large number of customers engage in Internet banking, the numbers are small compared to those who do not use Internet banking services. This low uptake is partly as a result of the nature of Internet banking, which involves the acquiring and processing of sensitive information, such as bank card numbers, personal identification numbers and passwords (Suh & Han 2002). Due to the sensitivity of banking information, privacy and security concerns often overshadow the benefits that Internet banking provides. It is, therefore, imperative for banks to comply with - and to abide by - recognised principles and policies that regulate the electronic environment, so as to protect consumers and build up much-needed levels of trust.

Consumer protection acts have been developed in many countries. In South Africa, consumers are protected by the Electronic Communications and Transactions (ECT) Act No. 25 of 2002. Banks and other businesses implement the ECT Act in terms of a privacy policy statement which they post on their website. A statement such as this specifies how the personal identifiable information that is collected from fields and forms during web-based transactions will be used by the site. A privacy policy statement is perceived as an important tool, by means of which banks provide evidence of their trustworthiness to their customers. Therefore, banks should have a privacy policy statement that adheres to the requirements of the ECT Act, in order to indicate their trustworthiness. This paper's purpose is twofold: firstly, to investigate South African Internet banking websites' compliance with the ECT Act and, secondly, to investigate customers' perceptions of bank privacy policy statements.

The rest of this paper is structured in the following way:

- Section 2 provides the background to Internet banking and privacy-related issues in South Africa.
- Section 3 presents a section of the ECT Act which is specific to the current study.
- Details of the implementation of the ECT Act are presented in Section 4.
- The research methodology which was used in the present study is described in Section 5.
- Section 6 presents the results of the study.
- Section 7 discusses the findings of the study.
- Section 8 provides the conclusions which have been drawn from the study.

CHALLENGES FACING ONLINE BANKING AND ONLINE-RELATED TRANSACTIONS

Internet banking in South Africa is estimated to have started in 1996. Many consumers have since taken advantage of the convenience, ease of use and relatively low cost of online banking (Singh 2004). Currently, the four major domestic retail banks all provide web-based Internet banking, as well as cellphone banking services, to their clients (Manson 2002). Recent statistics indicate that cellphone banking is the most popular mode of doing online banking in the country (Mobility 2009). The number of customers making use of such a service increased from 17% in 2007 to 28% in 2009. Whereas 10% of bank customers use cellphone and Internet banking, 6% use only Internet banking, 18% use only cellphone banking and 66% do not use any of these electronic channels (Mobility 2009).

SA Journal of Information Management
Article #418

The relatively low Internet banking adoption rates in South Africa are primarily due to the lack of Internet access and usage among the vast majority of the population. Only recently has the number of Internet users increased to 10% of the population, not all of whom use Internet banking services. Bank customers continue to be concerned about how their personal data are being used by the government and their banks (Singh 2004; Udo 2001). These concerns detract from consumer confidence and trust in Internet-related technologies and applications, such as Internet banking.

Trust is one of the key factors which is associated with successful Internet banking (Bradley, Brown & Patel 2007). Trust develops when the participants in a transaction feel secure and assured that only authorised users have access to information and that the quality of the information being accessed is complete, uncorrupted and easily accessible (McConnell 1994). Rotchanakitumnuai and Speece (2003) attribute consumer mistrust of Internet technologies to, amongst other things, the methods used for web security. These methods include electronic signatures, digital certificates, smart cards and biometrics. To counteract the perceived high costs of implementation, many banks choose not to implement at least some such security measures (Singh 2004). The failure to implement certain security measures can be detrimental to a bank's reputation, because the intention to make use of Internet banking services is partly affected by the users' perceptions of 'credibility regarding security and privacy issues; ability to provide the service, and possession of the necessary experience to build a reputation as a competent technology-based service provider' (Rotchanakitumnuai & Speece 2003; Wang *et al.* 2003). The banking sector cannot afford to tarnish its reputation, because a good reputation is 'one of the major factors that affect customer adoption of new technology-based service delivery' (Rotchanakitumnuai & Speece 2003). In response to such challenges (and specifically to customer concerns) governments have drafted legislation which is aimed at consumer protection. In South Africa, consumers are protected, as far as such delivery is concerned, in terms of the provisions of the ECT Act.

THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

The South African government views information technology as an enabler of economic development. South Africa has established itself as the leader in Africa's information communication and technology (ICT) market, in which the Internet has been commercially available since about 1994 (Brown & Buys 2005; Johnston *et al.* 2008); such a position of leadership has resulted in many ICT-related business applications becoming available, including Internet banking, which allows for consumers to have fairly wide-ranging control over their finances (Green & Van Belle 2003; Singh 2004). Whereas Internet banking provides several benefits, the government is aware of the rise in the levels of electronic abuse and computer-related crimes, such as identity theft, phishing, cyber-fraud (Kyobe 2009; Magele 2005). To address these problems, the government has introduced a set of laws aimed at regulating the electronic environment (Kyobe 2005; Singh 2004; Van Belle & Joubert 2004; Van Belle *et al.* 2004; Van der Merwe 2003). One such law is the ECT Act, which, among other objectives, strives to promote legal certainty and confidence in respect of electronic communications and transactions, as well as to safeguard personal information when such information is processed by public and private bodies (Kyobe 2009).

The ECT Act addresses all forms of electronic communication and other issues relating to cyber inspectors, service provider liability and domain names. The main purpose of the Act, though not exhaustive, is to provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for South Africa; to provide for human resource development in electronic transactions; to prevent abuse of information systems and to encourage the use of e-government services (South African Government, 2002). These objectives are elaborated on in the various chapters of the Act, of which there are 14 in total. Chapter 8 is of particular interest in terms of the topic of the current paper, which relates to the protection of personal information. Chapter 8 defines the scope of protection of personal information and provides guidelines in the form of principles (see Table 1) for electronically collecting personal information.

The scope of Chapter 8 is limited to only personal information which is obtained by means of electronic transaction. According to the Act, personal information can only be collected and used by a 'data controller', who is a person or organisation (e.g. as a bank) which electronically requests, collects, collates, processes or stores personal information from, or in respect of, a data subject. The data controller can voluntarily subscribe

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 the 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 to do so by law, or specifically authorised 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.

to those principles which are aimed at protecting the user's rights to privacy (Magele 2005). The making available of such information to the data controller concerned is subject to the relevant permission being granted by the person (data subject) from whom the personal information has been requested. If a data controller chooses to subscribe to the listed principles, the controller must subscribe to all of the principles concerned and not merely to some or parts, of them.

IMPLEMENTATION OF THE ECT ACT

The ECT Act is complied with by many businesses in terms of their websites' privacy policy statement (Van Belle & Joubert 2004). A privacy policy statement is a strategic tool that not only tackles privacy issues by stating how the site will use personal identifiable information that is collected from the data which are provided in response to certain fields and forms in web-based transactions (Gutwin & Levy 2005), but which also acts as a tool by means of which to increase customer trust (Arcand *et al.* 2007; Criswell *et al.* 2007). A statement such as this informs customers of the privacy practices of the business or organisation concerned and helps customers to make decisions regarding their business transactions by notifying them of how and why their information is being collected, how the information is to be used and to whom the information will be disclosed.

Furnell and Karwani (1999) found 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 those websites which displayed a privacy statement. Other studies have noted that 'people tend to purchase from merchants that offer more privacy protection and even pay a premium to purchase from such merchants' (Tsai, Egelman & Acquisti 2007). However, an overwhelming 80% of South African websites listed on the 'Proudly South African' website were found not to comply with the requirements of the ECT Act (Electronic Consultancy 2004). In 2002, only one company, kalahari.net, was found to be 100% compliant with the ECT Act (Pather, Remenyi & De la Harpe 2006). Even the banking sector which is a sector that deals with sensitive information and that should, therefore

> *provide a system that is sufficiently secure and that conforms to the technological standards that are acceptable for the type of transaction concerned, simply ignores the law and disclaim themselves of any and all liability*
>
> (Personal Finance 2006)

According to a survey which was conducted by Trust Online (a company that certifies website compliance with Internet-related legislation), the websites of the larger banks in South Africa are not yet fully compliant with the ECT Act. Some banks

> *do not provide consumers with sufficient ways of determining whether or not the website is safe and secure, notwithstanding statements made by those banks regarding security on their websites.*
>
> (Computer Business Review 2002)

RESEARCH METHODOLOGY

This study is mainly interpretive and followed two main research techniques: content analysis and interviews. Content analysis has been used in previous research concerning websites and privacy policies (Hooper & Johnston 2008). In the present study, content analysis was used to analyse the compliance of the websites of South African banks with the principles of Section 51 of Chapter 8 of the ECT Act. The data sample consisted of 13 banks. Although there were 36 registered banks in South Africa at the time of the study, the study focused only on South African controlled banks, of which there were only 14. Of the 14 in question, one was under curatorship and no longer had a website available. As a result, 13 banks were assessed in the current study.

Based on the content analysis, an interview guide was developed to guide the collection of information in interviews regarding users' interpretations and perceptions of privacy policy statements. We specifically investigated the users' perceptions of said policy's accessibility, understandability and readability. The interview also investigated users' awareness of the ECT Act and their perceptions of those banks that do not comply with the requirements of the ECT Act. All the interviews were semi-structured, which provided sufficient flexibility for those issues which were not covered by the predefined interview questions to emerge during the interviews. The issues concerned were then subjected to further exploration. Ten Internet banking users were interviewed as part of the study. The researchers who are responsible for the current study are aware of the small size of the sample, but the interpretive nature of the study should be borne in mind. The research concerned does, therefore not restrict itself to such generalisation as would have been possible if the study had been strictly based upon statistical sampling. Interpretivist research does not 'prohibit the researcher from extending his or her theory to additional settings', but, instead, allows for generalisation in its own right (Lee & Baskerville 2003).

RESULTS AND ANALYSIS

Compliance with the ECT Act

The results of the content analysis indicate that 69% of the South African banks sampled posted a privacy policy statement on their website. Some of these banks stated the importance of customers reading their privacy policy statement prior to their registering as an Internet bank user. The remaining banks lacked a privacy policy statement, as well as any other means of conveying privacy-related issues to their customers. The specific concern of the current study related to the extent to which the 69% of banks earlier identified satisfied all nine principles of the Act. The findings indicated that, of those banks which had a privacy policy statement, none adhered to all the principles prescribed by the ECT Act.

For example, in terms of Principle 1 of the ECT Act (see Table 1), which requires that the express written permission of the customer be obtained, it was found that, in order to obtain the consent of the customer, some banks inserted a clause which stated that, by reading the privacy statement, the customer, in effect, was agreeing to share their personal information with third parties. The clause inserted by the banks does not equate with the 'express written permission of the data subject', because the users do not provide their written consent to the sharing of such information. Written consent does not have to be provided in the form of actual written documents, however, but can be in the form of a checkbox, which the user can check to indicate that the relevant permission is granted, with the information being stored in such a form.

Some banks also did not comply with Principle 4, which prevents banks from using a customer's information for any purpose other than that which is stated in their privacy statement. Only 15% of the banks concerned gave the customers the option of giving their consent for the use of their personal information for other purposes. Although most of the banks did state that they would not share customer information with third parties, they also indicated that, in some circumstances, they would be prepared to share customer information 'to protect the Company's rights'. They, however, were found not to indicate that they would inform the customers affected by such a scenario.

Readability and understanding of privacy statements

The content analysis results showed that all the privacy statements were complex, difficult to read and lengthy. The analysis was augmented with the application of the Flesch Readability scale, which assigns a score on the basis of the minimal grade

SA Journal of Information Management Article #418

level required to read and understand English text. The Flesch Readability scale is automated in Microsoft Word and has been demonstrated to be reliable and valid (Paasche-Orlow, Taylor & Brancati 2003).The readability ease scores which were obtained for the current study are depicted in Table 2. The higher the Flesch Reading ease score (with, for example, a score of approximately 60 to 70 being regarded as relatively high), the more readily understandable the text concerned should be. The Flesch–Kincaid scale was chosen because of its convenience and its availability for computerised use, seeing that it is embedded in Microsoft Word. In the current study, all the privacy statements which were supplied by the banks surveyed obtained a Flesch score of between 20 and 45, indicating that the statements concerned ranged in ease of readability and understandability from difficult to very difficult. The wording of such statements, which included such words as 'cookies' and 'encryption', would often have been difficult for a customer who lacks a technological background to understand and could easily have led to confusion and misinterpretation. However, some banks did define the more complex terms that they used.

None of the banks surveyed posted their privacy statements in any of the South African official languages other than English. Customers whose first language is not English would, consequently, have found it relatively difficult to comprehend such statements. The interviewees felt that the clarity of the content was important, in order to prevent misunderstanding. As was indicated by one respondent,

> *the easier it is to understand the policy, the easier it is to trust. If they were very clear and specific, then I would trust them more. Whereas if they covered themselves by being vague, then I would wonder why the vagueness, and I* [would] *probably lose trust.*
>
> (Respondent)

In addition to being difficult to read, the statements tended to be lengthy and 'time consuming'. These failings deterred consumers, especially those who were unfamiliar with the ECT Act, from reading them. One respondent stated 'it's just too long and complicated ... I don't have to read it, because someone makes sure it is up to standard.'

Accessibility of privacy statements

In investigating the accessibility of the privacy policy statements concerned, specific attention was paid to the exact location of the privacy policy statements on the banks' websites. Table 3 indicates where the privacy policy statements were located for the different banks investigated. Twenty-three per cent of such statements were displayed on the bank's home page, which made them relatively easy to access. However, 77% of the statements were difficult to find, as they were posted under one of the following sections:

- terms and conditions
- disclaimer
- legal requirements
- privacy and security.

These locations necessitate further navigation by the user, which many users could find tedious. Most policy statements were located at the bottom of a web page and were usually

TABLE 2
Flesch Reading Ease score for South African banks' Privacy Statements

	Total	Flesch		Readability
Bank	Words	Score	Grade level	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	Difficult
G	1143	30.7	16.2	Difficult
H	244	35	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

TABLE 3
Location of the privacy policy statement on the banks' website

Section under which statement posted	Bank
Privacy & security	A ; B ; G
Terms & conditions	D ; L
Legal requirements	D ; L
Disclaimer	D ; L
Legal requirements: disclaimer	H
Legal requirements: privacy & security	J
Terms & conditions & Legal requirements	E

accessible via a link (e.g., by clicking on a button for 'Terms and Conditions'). Although the respondents agreed that such a location was suitable in terms of consistency, as supported by Jensen and Potts (2004), they also felt that by assigning such a location to the statement, 'the impression is that the privacy statement is not that important'

Customer awareness of the ECT Act

Less than 45% of the respondents in the current study were aware of the ECT Act, of privacy statements and, specifically, of the protection of personal information. Some of the respondents indicated irritation with companies that did not comply with the ECT Act. One of the respondents stated:

> *I have been receiving calls from a company that I am not aware of, and I have no idea where they got my contacts from. I mean, they know my cellphone number and name – everything! I asked them where they got my details, and they didn't tell me, which makes me believe they are not compliant with the ECT Act. Even if I wanted services from that company, I just can't trust them. From this experience, I started doubting the companies I am currently getting my services from – including my bank. It has to be one of them that gave that company my information – I am getting suspicious.*
>
> (Respondent)

Feelings of mistrust, suspicion and irritation were found to be general among the group of respondents which was familiar with the ECT Act. The respondents concerned reported feeling that those companies which do not adhere to the principles and guidelines of the ECT Act should not post a privacy policy statement on their websites, as such posting then erroneously leads customers to believing that they are compliant with the Act.

The other 55% of respondents stated that they were unsure and even, in some cases, unaware of the existence of a privacy statement on their bank's website. They were also not familiar with the ECT Act. They, however, did indicate that it was important for banks to post a privacy statement on their website, because, as clients, they would then be able to assess the bank's trustworthiness and

> *it would show what the banks were going to use the information for ... it would show the implications of using the Internet [bank] with regards to disclosure of personal information.*
>
> (Respondent)

Both of the above-mentioned groups indicated that banks which disclose information to third parties without the consent of the customer should be penalised for doing so, for the following reason:

> *That is very misleading, and it is very unethical for them to do so. It will most probably destroy my confidence in the bank . . . 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.*
>
> **(**Respondent**)**

DISCUSSION

Both online and mobile Internet-related transactions are not a new phenomenon in South Africa. Although Internet users are

eager to adopt such technology, the consumers still perceive the risks associated with privacy and security to be inhibiting. To address their fears, banks and many organisations use privacy policy statements to indicate their compliance with the ECT Act, which is intended to protect their customers' personal information from being used illegally, sold or shared with third parties without the individuals' consent.

The current study showed that, although 69% of the South African banks sampled did post a privacy policy statement on their website, none of them adhered to all the requirements of the ECT Act concerning their customers' personal information. These findings are of concern to consumers, because those banks which lack a privacy policy statement tend to increase consumer risks associated with Internet banking. In the interviews, the respondents indicated that, if their bank did not have a privacy policy on their website, they would not use their Internet banking services. Some indicated that they would rather 'switch to a bank that has a privacy policy statement'. These findings are consistent with those of Bradley *et al.* (2007), who found that a lack of structural assurances (such as privacy policy statements) has a major influence on the levels of trust experienced, which, in turn, impacts on the adoption and usage of Internet banking services.

A significant number of the respondents interviewed were not aware of the ECT Act, but were aware of the existence of privacy policy statements. These respondents assumed that all banks adhered to the rules of Internet banking set down by governing bodies. The same perceptions were held by those respondents who indicated some understanding of the ECT Act and of what a privacy policy entails. These findings were consistent with those of Egelman *et al.* (2006), who state that 'few users make the necessary effort to read privacy policies, let alone seek out the websites that have the best privacy policies'. Those participants who were unaware of the ECT Act, for example, were not aware that a data controller who chooses to subscribe to the listed principles in Table1 must subscribe to all of the principles concerned and not merely to some. Because of their lack of awareness, many consumers assume that a policy statement on the website is sufficient evidence that a bank adheres fully to the ECT Act. As has already been mentioned, the undue length and complex terms used in the policy statements make it difficult for consumers to interact with them. These findings are consistent with those of Caudill and Murphy (2000), who state that 'even with the disclosure of privacy statements, confusion can arise from the vague and often ambiguous nature of some of them'.

Banks have a responsibility to make their policies clear and unambiguous to their customers. To achieve this, banks should take into account the reading preferences of consumers. South Africa is a multilingual country. As their home language, more than 78% of South Africans speak an African or other vernacular language, 13% speak Afrikaans and only 8% speak English. Most of the population prefers to communicate in their vernacular language and often resort to switching between the vernacular and English in their communication (Howie & Scherman 2008). As a result, some users of Internet banking may be unable to comprehend in full a privacy policy which is in English and which contains complex technological jargon. To ensure that privacy policy statements are easily understood by all Internet banking users, banks should allow their online customers the option to choose the language in which they would like to view the privacy policy. An allowance such as this would help to ensure that banks promote and respect all those languages which are commonly used by South African communities.

Those respondents who were aware of the ECT Act and of security and privacy policies, were disheartened to find that some banks adhered to only some of the ECT Act principles, instead of to all, as is required of them. Those banks which do not adhere to all the ECT Act principles could be doing so in order to avoid incurring the costs which are associated with meeting such requirements. It might also be that

> *most information security practitioners are not familiar with sections that deal with security-related aspects in this Act and as such very few security experts and practitioners incorporate the Act's security requirements in the IT policies.*
>
> (Dagada, Eloff & Venter 2009)

The information security practitioners' lack of awareness of the security-related aspects to do with such policies might be the result of the Act itself lacking 'detail on how it will encourage the private sector to participate' (ITWeb 2010). Whatever the reasons for the failure of many banks to comply with the prescribed regulation, the respondents in the current study indicated that such banks jeopardise the relationship of trust which they are meant to have with their customers. When customers lack confidence in their bank, they are likely to switch to a different bank, or to take such drastic steps as, according to one interviewee, to 'challenge them in court'. Banks need to ensure that, if they have decided to comply with the principles which are set down in the ECT Act, they should comply with all of them and not merely some in order to boost consumer confidence and to avoid litigation. Van Dyke, Midha and Nemati (2007) indicate that privacy empowerment has a strong influence on issues relating to both privacy concern and trust in electronic transactions. Therefore, banks should consistently strive to ensure that they meet the requirements of the ECT Act if they have opted to adhere to the principles set out in it.

To facilitate compliance with the Act, there is a need for regulatory bodies, such as the Banking Association of South Africa, which is responsible for 'establishing and maintaining the best possible platform on which banks can do responsible, competitive and profitable banking' (Banking Association South Africa n.d.) to educate their members accordingly. Another regulatory body which is of relevance to the protection of consumer privacy is the South African National Payment System, which manages all systems, institutions, agreements, procedures, rules, laws and mechanisms for the clearing of such payments as cheques and electronic and card payments between banks (The national payment system in South Africa 2005). Regulatory bodies can serve as watchdogs for customers, helping to ensure that the privacy policy statements of banks that use Internet banking fully comply with the requirements of the ECT Act.

CONCLUSION

The need to secure and protect consumers' private information has led to the use of privacy policy statements, which state the different ways in which a website may use personal identifiable information online. Many bank websites carry a privacy policy statement, which can be used as a strategic tool for increasing levels of customer trust and confidence in the bank concerned. However, such privacy policy statements need to meet those conditions governing Internet-related transactions which are set out in the ECT Act.

The study described in this paper found that most banks have a privacy policy statement which is posted on their websites. However, these statements do not always meet all of the requirements which are set out in the ECT Act. In addition, most statements are not easily accessible to the user and are presented in a variety of language which is neither easily accessible to, nor readily understood by, some non-English speakers. The lack of readability of the privacy statements poses another problem, in terms of the complex terms used and the excessive length of the statements. In the study, customers indicated the importance of every bank having a privacy policy statement and the importance of such a policy meeting the requirements of the ECT Act. Customers believe that, if the policies concerned were to meet the requirements, they would be more likely to trust the banks concerned, which would build their business confidence.

The study found that those banks which do not adhere to the provisions of the ECT Act detract from business confidence, leading to customer doubt and scepticism concerning all facets of these banks.

The current researchers draw the following conclusions from this study:

- All South African banks that provide Internet banking services should have a privacy policy statement that is easily available to their customers.
- Banks should consider making their privacy policy statements available in all South Africa's official languages, rather than just in English. The respondents in the study indicated that making such statements available in the home language of all their customers would benefit those customers whose home language is other than English.
- There is a need for a regulatory body to review the privacy policy statements of those banks which use Internet banking, in order to ensure that such banks comply fully with the requirements of the ECT Act.

Future research needs to investigate the reasons for banks noncompliance with all the requirements of the ECT Act. There is scope for more research into technologies which should help enhance the levels of protection of privacy in the South Africa market. Further research into such areas should help South African banks to boost the levels of customer trust and business confidence in them. The current study has limited its investigation to web-based Internet banking. Given that cellphone banking has surpassed web-based Internet banking as the online medium of choice, future research should investigate the compliance of banks with legal requirements regarding their cellphone offerings.

REFERENCES

Arcand, M., Arle-Dufour, M., Nantel, J. & Vincent, A., 2007, 'The impact of reading a website's privacy statement on perceived control over privacy and perceived trust', *Online Information Review*, 31(5), 661–681.

Banking Association South Africa, n.d., *The Role of The Banking Association South Africa*, viewed 16 September 2009, from http://www.banking.org.za.

Bradley, L., Brown, I. & Patel, K., 2007, 'The antecedents and consequences of trust in Internet banking', in *Proceedings of the 9th annual conference on WWW applications*, Johannesburg, September 5–7, 2007, pp. 1–13.

Brown, I. & Buys, M., 2005, 'A cross-cultural investigation into customer satisfaction with Internet banking security', in *Proceedings of the 2005 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, pp. 200–207.

Caudill, E.M. & Murphy, P.E., 2000, 'Consumer online privacy: Legal and ethical issues', *Journal of Public Policy & Marketing*, 19(1), 7–19.

Cazier, J.A., Shao, B.B. & St Louise, R.D., 2003, 'Addressing e-business privacy concerns: The role of trust and value compatibility', *ACM symposium on applied computing*, ACM, Melbourne, pp. 617–622.

Cheng, E.T.C., Lam, D.Y.C. & Yeung, A.C.L., 2006, 'Adoption of Internet banking: An empirical study in Hong Kong', *Decision Support Systems*, 42, 1558–1572.

Computer Business Review, 2002, *SA bank websites not safe and compliant*, viewed 25 February 2010, from http://www.cbr.co.za.

Criswell, J., Crossland, M., Meinart, D. & Peterson, D., 2007, 'Customer trust: Privacy policies and third-party seals', *Journal of Small Business and Enterprise Development*, 14(4), 654–699.

Dagada, R., Eloff, M.M. & Venter, L.M., 2009, 'Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?', in *Proceedings of the 8th annual information security South Africa conference*, Johannesburg, July 6–8, 2009, viewed 5 April 2010, from http://icsa.cs.up.ac.za/issa/2009/Proceedings/Full/4_Paper.pdf.

Egelman, S., Tsai, J., Cranor, L.F. & Acquisti, A., 2006, 'Studying the impact of privacy information on online purchase decisions', in *Proceedings of 2006 CHI privacy methods workshop*, Montreal, Quebec, Canada, 2006, viewed 12 May 2009, from http://cups.cs.cmu.edu/pubs/chi06.pdf.

Electronic Consultancy, 2004, *Compliance to the ECT Act*, viewed 12 May 2009 , from http://elc.co.za.

Furnell, S. & Karweni, T., 1999, 'Security implications of electronic commerce: A survey of customers and businesses', *Internet Research*, 9(5), 372–382.

Green, S. & Van Belle, J.P., 2003, 'Customer expectations of Internet banking in South Africa', in *Proceedings of the third international conference on electronic business (ICEB)*, Singapore, 9-13 December 2003, pp. 283-285.

Gutwin, C. & Levy, S.E., 2005, 'Improving understanding of website privacy policies with fine grained policy anchors, *International World Wide Web conference*, ACM, Chiba, Japan, May 10–14 pp. 480–488.

Hooper, A.C.S. & Johnston, K.A., 2008, 'Establishing business integrity through website statements – an exploration of South African banking websites', in *Proceedings of the 10th annual conference on World Wide Web applications*, 2008, University of Cape Town, Cape Town, South Africa, September 3–5, 2008

Howie, S. & Scherman, V., 2008, 'The achievement gap between science classrooms and historic inequalities', *Studies in Educational Evaluation*, 34, 118–130.

ITWeb, 2010, *Draft cyber policy welcomed, criticized*, viewed 25 May 2010, from http://www.itweb.co.za.

Jayawardhena, C. & Foley, P., 2000, 'Changes in the banking sector – the case of Internet banking in the UK', *Internet Research*, 10(1), 19–31.

Jensen, C. & Potts, C., 2004, 'Privacy policies as decision-making tools: An evaluation of online privacy notices', in *Proceedings of the SIGCHI conference on human factors in computing systems*, Vienna, Austria, April 24–29, pp. 471–478.

Johnston, K.A., Kabanda, S.K., Adams, S. & Davids, E., 2008, 'How SMEs in Western Cape of South Africa use ICT', in *Technology management for a sustainable economy: Management of Engineering & Technology, PICMET 2008, Portland international conference*, ieeexplore July 27–31, 2008, pp. 1043–1051.

Kyobe, M., 2005, 'Addressing e-crime and computer security issues in homes and small organizations in South Africa', *European management and technology conference on the integration of management and technology*, Citeseer Rome, Italy, pp. 1–13.

Kyobe, M., 2009, 'Factors influencing SME compliance with government regulation on use of IT: The case of South Africa', *Journal of Global Information Management*, 17(2), 30–59.

Lee, A.S. & Baskerville R.L., 2003, 'Generalizing generalizability in information systems research', *Information Systems Research*, 14(3), 221–243.

Liu, C. & Arnett, K.P., 2000, 'Exploring the factors associated with website success in the context of electronic commerce', *Information & Management*, 38, 23–33.

Magele, T., 2005, *E-security in South Africa*, White Paper prepared for the ForgeAhead E-Security event, 16/17 February 2006.

Manson, H., 2002, 'Driving home value to banking customers', *Journal for Convergence*, 2(5), viewed 13 January 2003, from http://www.itweb.co.za/sections/business/2002/0205271217.asp.

McConnell, J., 1994, *National training standard for information system security*, viewed 21 January 2009, from http://www.nstissc.gov/Assets/pdf/4011.pdf.

Mobility, 2009, Mobility 2009 reveals SA's cellular gap. 2009, viewed 6 April 2010, from http://www.mobileza.com.

The national payment system in South Africa, 2005, viewed viewed 6 April 2010, from http://www.reservebank.co.za.

Paasche-Orlow, M.K., Taylor, H.A. & Brancati, F.L., 2003, 'Readability standards for informed-consent forms as compared with actual readability', *New England Journal of Medicine*, 348(8).

Pather, S., Remenyi, D. & De la Harpe, A., 2006, 'Evaluating e-commerce success: A case study', *Electronic Journal of Information Systems Evaluation*, 9(1), 15–26, viewed 23 June 2009, from http://www.ejise.com.

Personal Finance, 2006, *Banks 'fail' to protect online clients*, viewed 17 February 2009, from http://www.persfin.co.za/index.php?fArticleId=3328888.

Rotchanakitumnuai, S. & Speece, M., 2003, 'Barriers to Internet banking adoption: A qualitative study among corporate customers in Thailand', *International Journal of Bank Marketing*, 21(6/7), 312–323.

Singh, A.M., 2004, 'Trends in South African Internet banking', *Aslib Proceedings: New Information Perspectives*, 56(3), 187–196.

South African Government, 2002, Electronic Communications and Transactions Act, viewed 3 February 2009, from http://www.internet.org.za/ect_act.html.

Suh, B. & Han, I., 2002, Effect of trust on customer acceptance of Internet banking, *Electronic Commerce Research and Applications*, 1(3/4), 247–263.

Tsai, J., Egelman, S. & Acquisti, A., 2007, 'The effect of online privacy information on purchasing behavior: An experimental study', paper presented at *6th workshop on the economics of information security (WEIS)* , Carnegie-Mellon University, Citeseer, June 2007.

Udo, G.J., 2001. 'Privacy and security concerns as major barriers for e-commerce: A survey study', *Information Management and Information Security*, 9(4), 165–174.

Van Belle, J.P. & Joubert, J., 2004, 'Compliance of South African e-commerce websites with legislation to protect *customer* rights', in *Proceedings of the 2004 international business information management conference (IBIM '04)*, International Business Information Management Association (IBIMA) Amman, Jordan 4–6 July 2004, pp. 437–446.

Van Belle, J.P., Haig, A., Mitchell, C. & Watson, M., 2004, 'Data privacy and customer protection in South African e-commerce', in *Proceedings of the annual information technology congress (CATI '04)*, FGV, EAESP, São Paulo (Brasil), June 2004, pp 22–25.

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?', Honours thesis, Dept. of Information Systems, University of Cape Town, Cape Town, South Africa.

Van Dyke, P.T., Midha, V. & Nemati H., 2007, 'The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce', *Electronic Markets*, 17(1), 68–81.

Wang, Y.S., Wang, Y.M., Lin, H.H & Tang, T., 2003, 'Determinants of user acceptance of Internet banking: An empirical study'. *International Journal of Service Industry Management*, 14(5), 501–519.

SA Journal of Information Management
Article #418