

Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa

Benson Zenda , Ruthea Vorster , Adéle Da Viega 

School of Computing, University of South Africa, South Africa

ABSTRACT

South Africa enacted the Protection of Personal Information Act 4 of 2013 (POPI) in an effort to curb the misuse of customers' personal information by organisations. The aim of this research was to establish whether the South African insurance industry is adhering to certain prescripts of POPI, focusing on direct marketing requirements. An experiment was utilised to monitor the flow of personal information submitted to 20 insurance companies requesting short-term insurance quotations, using new e-mail addresses and phone numbers. The results of the experiment indicate that 92% of the marketing communication received did not have prior consent from the researcher. Contact was made by companies outside the sample, indicating third-party sharing. 86% of the unsolicited short message service (SMS) communication received required customers to pay for unsubscribing from SMSs, which is not in line with regulatory requirements. The non-compliance evident in this experiment acts as an early warning to the insurance industry and South Africa, prompting a more concerted effort towards preparation of compliance with POPI. A personal information processing management framework is proposed to aid the insurance industry in understanding how personal information can be processed in line with the requirements of the Act.

Keywords: direct marketing, personal information, privacy, Protection of Personal Information Act (POPIA), privacy framework, personal information processing management framework (PIPMF)

Categories: • Security and privacy ~ Privacy protections

Email:

Benson Zenda benson.zenda@kznccogta.gov.za (CORRESPONDING),
Ruthea Vorster rvorster@unisa.ac.za,
Adéle Da Viega dveiga@unisa.ac.za

Article history:

Received: 7 Jun 2019
Accepted: 18 Mar 2020
Available online: 20 Jul 2020

Zenda, B., Vorster, R. and Da Viega, A. (2020). Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. *South African Computer Journal* 32(1), 113–132. <https://doi.org/10.18489/sacj.v32i1.712>

Copyright © the author(s); published under a [Creative Commons NonCommercial 4.0 License \(CC BY-NC 4.0\)](#).
SACJ is a publication of the South African Institute of Computer Scientists and Information Technologists. ISSN 1015-7999 (print) ISSN 2313-7835 (online).

1 INTRODUCTION

The availability of vast amounts of customer information—also referred to as big data (K. D. Martin & Murphy, 2017)—has resulted in companies utilising psychological targeting (Matz et al., 2020) and marketing analytics to focus marketing communication to specific groups of customers. The marketing communication via electronic mail or SMS is based on obtaining permission from the customer (Hartemo, 2016). To gain competitive advantage, companies collect and analyse customers' personal data mostly for customisation or alignment of products to specific customers' needs (Curry, 2016). This analysis and use of data increases productivity through improved business intelligence and, furthermore, the main business goal of some companies is the generation and sale of data (European Commission, 2013). This implies that customers' personal information is an important commodity for a strategic advantage. Personal information is now viewed as a tradeable commodity and markets for such information are emerging (Spiekermann et al., 2015). Collected personal information can contain important contact information, such as mobile numbers, telephone numbers and e-mail addresses. This information can be used by companies to contact potential and current customers to sell goods and services. This is regarded as unsolicited marketing communication and is viewed by customers as an invasion of their privacy (Krafft et al., 2017). The perceived value of customer information can lead to cybercrime, such as fraud, hacking of organizations databases to obtain customer information, unsolicited emails and ultimately customer privacy invasion (K. D. Martin & Murphy, 2017). In an effort to minimize the concerns relating related to security, privacy and fraud, it is imperative that countries pass laws to protect against the abuse of personal information collected during normal business transactions.

In South Africa, the enactment of the Protection of Personal Information Act 4 of 2013 (POPIA) (RSA Government, 2013), provided relief to customers whose personal information was being utilised by companies for purposes such as direct marketing of services and goods without their consent. Section 69 of POPIA prohibits the use of collected personal information as a source of information for direct marketing of goods and services, unless there is consent by means of an opt-in for new customers who may only be contacted once, or, if existing customers are contacted for similar products or service, by giving them the option to opt out. It is therefore imperative that regulatory requirements concerning the protection of personal information should be considered when personal information is utilised for marketing purposes. Although South Africa now has privacy legislation to protect personal information processed by companies, it must be established whether the companies are adhering to the privacy conditions stipulated in this Act when marketing goods and services to individuals.

Although POPIA is on par with international privacy legislation, surveys undertaken indicate that only 40% of companies in South Africa have started processes to comply with POPIA (Baloyi & Kotze, 2017; Grobler et al., 2015). It can be argued that such low levels of POPIA compliance preparedness can result in companies contravening POPIA prescripts; specifically, of concern in this research, is section 69(1), which prescribes that the use of personal information for direct marketing is prohibited unless the data subject has given permission to the

responsible party.

The commencement date for POPIA will be proclaimed by the President through a gazette and different commencement dates may be announced for different classes of information holders. Although the date of commencement has not been announced, it can be argued that the announcement is imminent as the act was promulgated in 2013. Once the commencement date is announced, organisations will have one year in which they must adhere to POPIA prescripts (RSA Government, 2013). Organisations must utilise the time before the commencement date to put in place processes that aim to minimise the risk of contravening any prescripts of POPIA (de Bruyn, 2014).

The aim of this research project is to establish the extent to which insurance companies are adhering to the requirements of POPIA when marketing services and goods to potential customers. Online insurance quotations were obtained by depositing personal information on the websites of twenty insurance companies. The flow of personal information emanating from the deposited information was then monitored to assess adherence to POPIA.

This research contributes to illustrate how personal information is being utilised and shared in the insurance industry. It is evident that some provisions of POPIA relating to direct marketing are being violated by South African insurance companies and hence require enforcement. The recommendations can be considered by the insurance industry to aid compliance.

2 RESEARCH AIMS AND QUESTIONS

This research aims to establish whether the South African insurance industry complies with the direct marketing requirements of POPIA. A personal information processing management framework (PIPMF) is proposed to aid organisations to implement the recommendations.

Section 69 of POPIA prohibits any marketing that is directed towards customers that have opted out from receiving marketing communication. Companies may contact potential customers once, to establish whether they prefer to opt in or opt out from receiving marketing communication. Thereafter, POPIA prohibits direct marketers from sending marketing communication to customers that have opted out from receiving marketing communication. The main research question is as follows:

Do insurance companies in South African only contact prospective customers if they have agreed to receive marketing communication, as specified by POPIA?

A literature overview is presented in Section 3 on information privacy and POPIA. The PIPMF is proposed in Section 4. The research methodology used in this study is presented in Section 5 and then followed by findings and discussions in Section 6. Finally the conclusion, limitations of the study and future opportunities for research are presented in Section 7.

3 LITERATURE REVIEW

The manner in which organisations process personal information can result in an increase in privacy concerns among customers (Xu et al., 2011). Privacy concern is prominent due to the large amounts of personal information that businesses collect, and the fact that customers generally lose control of the personal data that they provide to companies (Akhter, 2014). Personal information privacy has now become a major concern among most customers (Smith et al., 2011). This increased concern about how companies deal with information may have a negative impact on e-commerce (Wu et al., 2012), which relies heavily on customers disclosing their personal information online. Such negative perceptions and privacy concerns can be addressed by asking for permission before engaging in any direct marketing. Customers are more comfortable with communication that they have agreed to and view unsolicited messages as an intrusion into their privacy (Krafft et al., 2017). The introduction of POPIA in South Africa will allay such concerns if the Act is properly implemented (Skolmen & Gerber, 2015). It is therefore imperative that POPIA compliance be monitored closely to minimise the negative impact that customer privacy concerns may have on e-commerce. In the next subsection, an overview of privacy legislation is given.

3.1 Overview of privacy legislation

There has been a global increase in the number of legislations aimed at protecting personal information (Botha et al., 2017). Between 1973 and 2017, new data privacy laws have been enacted at a rate of 2.7 new countries annually; resulting in the enactment of more than 120 laws worldwide (Greenleaf, 2017).

In the European Union (EU) for example, the General Data Protection Regulation (GDPR) (2016) came into effect on 25 May 2018. The GDPR focuses on natural persons with respect to the processing of personal data and free movement thereof. To curb the negative impacts of globalisation and technological advancement on personal data, section 101 of the GDPR prescribes that personal data transferred from a data subject in the EU by an organisation outside the EU shall be conducted in a manner that fully complies with the GDPR. In the United Kingdom (UK), the Data Protection Act (DPA) (1998) regulates the processing of personal information. In the United States of America (USA), the 1973 Fair Information Practice (FIP) document describes the privacy rights of individuals to sensitive data. The FIP culminated in the 1974 Privacy Act, which embodies most of the principles from the FIP document. It should be noted that this Act only applies to data collected by government institutions. The USA is different from other cases cited, because it has enacted separate laws by data type, for example, a privacy law for healthcare information. The USA also allows individual state governments to regulate some aspects of privacy, which has resulted in variations between states, making it difficult to respect privacy laws of every state (Pfleeger et al., 2011).

Africa has generally lagged behind in respect of the adoption of data protection laws when compared to the rest of the world (Abdulrauf & Fombad, 2016). Significant work still needs

to be done in order to combat information privacy violations in African countries (Borena et al., 2015). Figure 1 shows the African countries that have privacy legislation, from a study conducted by Greenleaf (2017). Twenty out of the 54 African countries have enacted data privacy legislation (Greenleaf, 2017). This implies that only 37% of African countries have data privacy laws. On 27 June 2014, Africa demonstrated its commitment towards protecting individuals' personal information by adopting the African Union Convention Cyber Security and Personal Data Protection (AU Convention) (2014). The AU Convention seeks to compel member states to establish a legal framework to protect personal data. Furthermore, the AU Convention prescribes that the legal framework shall ensure that the fundamental freedom and rights of individuals are respected when personal information is processed. The AU Convention is aimed at harmonising previous regional and local data privacy initiatives in Africa (Abdulrauf & Fombad, 2016).

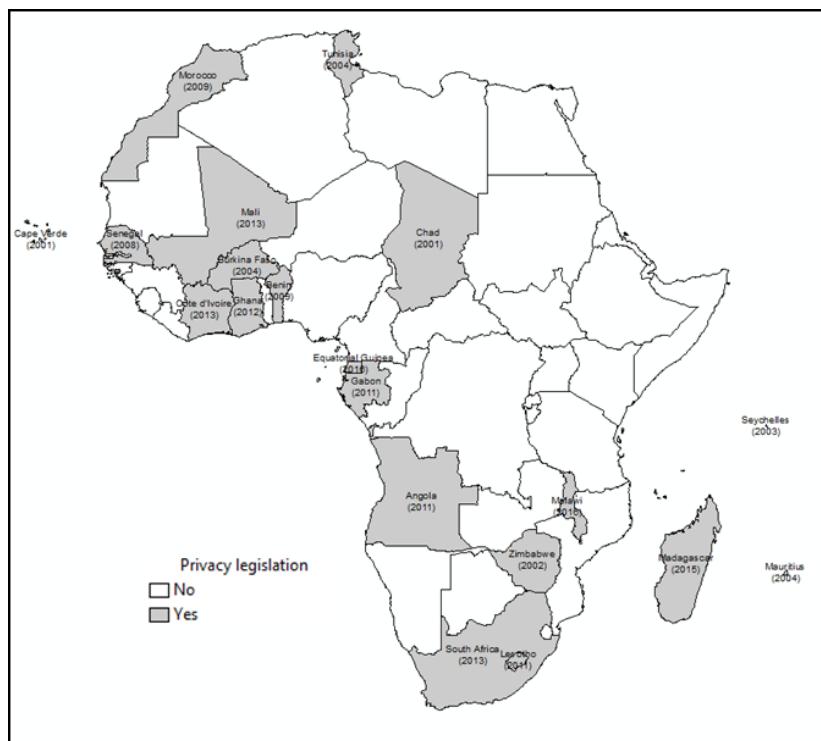


Figure 1: Map showing the spatial distribution of African countries with privacy legislation and the year of enactment (Greenleaf, 2017)

In South Africa, the Constitution of the Republic of South Africa (CSA) ((RSA Government, 1996)), grants all citizens a right to privacy in section 14. The Consumer Protection Act of South Africa (CPA) 68 (2009), further supports this constitutional right by highlighting in section 11 that every individual has a right to accept, stop or refuse communication intended to market services and goods directly. POPIA (2013) was promulgated to further uphold the con-

stitutional right to privacy by protecting personal information when processed by responsible parties. The next subsection gives an overview of POPIA.

3.2 Overview of the Protection of Personal Information Act 4 2013

The Protection of Personal Information Act 2013 (POPIA) defines a data subject as somebody to whom the personal information belongs. It further defines a responsible party as a private or public entity or individual who decides the purpose of and manner in which information that is personal in nature is processed. POPIA comprises eight conditions, as specified in Table 1, that should be satisfied before personal information can be processed lawfully.

Table 1: Eight conditions of POPIA as adapted from RSA Government (2013)

Condition	Description
Accountability	The Act prescribes that it is the onus of the responsible party to establish an environment that facilitates the lawful processing of personal information.
Processing limitation	The Act specifies that the processing of personal information can only commence if the purpose specifies the required information for an activity to be accomplished. The information should be sourced from the data subject directly.
Purpose specification	The Act specifies that information of a personal nature should be collected for a lawful, specific and clearly spelt-out purpose related to the mandate of the responsible party.
Further processing limitation	Further processing of information must be directly linked with the purpose of collection as per the initial agreement with the data subject.
Information quality	The responsible party has to guarantee that personal information is accurate, complete and not misleading.
Openness	It should be brought to the attention of individuals that a responsible party is collecting personal information from them.
Data subject participation	POPIA specifies that a data subject should be allowed to access information that they have supplied and be able to make corrections to it.
Security safeguards	It is the onus of the responsible party to put in place measures that ensure that the confidentiality and integrity of the information is preserved.

In addition to the eight conditions POPIA also includes provisions relating to direct marketing and unsolicited electronic communication which were specifically included in the scope and tested in this experiment.

The POPIA principles are in harmony with those of other leading countries, as highlighted by work conducted by Botha et al. (2017).

3.3 Privacy legislation and direct marketing

Potential customers can be accessed via messages that are relevant and tailor-made to individuals (Krafft et al., 2017). Most legislation opposes unsolicited direct marketing. Direct marketing is a way to approach a person using mail, face-to-face or an electronic method for the purpose of indirectly or directly promoting or supplying any goods or services (Abdulrauf & Fombad, 2016). Every individual has a right to stop a responsible party from utilising their personal information for marketing services and goods directly (UK Government, 1998). Similarly, section 30 of the EU Directive stipulates that individuals can refuse, without giving reasons, to have their personal information used for marketing services and goods directly. Every individual has a right to accept, stop or refuse communication intended to market services and goods directly (RSA Government, 2009). This is reinforced by section 69 of POPIA that prohibits the use of collected personal information for the purpose of sending direct marketing communication to a data subject, unless the data subject consents to such an arrangement. POPIA further emphasises that any communication intended to market goods and services directly to customers should have details of the person who sends the communication, to allow the receiver to send a request seeking the stopping of such communication. It is apparent from the above discussions that direct marketing is a necessity in the business world, but should be regulated to protect customers. Customer concerns on privacy can be addressed by meeting legal requirements and asking for permission before engaging in any direct marketing (Krafft et al., 2017).

3.4 Insurance industry privacy legislation in South Africa

The insurance industry in South Africa is regulated by three main Acts, namely the Short-term Insurance Act 53 (SIA), the Long-term Insurance Act 52 (LIA) and Insurance Act 18 (IA) (1998a, 1998b, 2017). Section 55 of the SIA defines direct marketing as offering and/or selling a policy by way of electronic mail, telephone and media inset and further defines a direct marketer as an insurer who conducts business using direct marketing. Section 55 of the SIA stipulates how a direct marketer should interact with a client, but lacks emphasis on the issue of privacy of personal information. Both the SIA and LIA therefore lack emphasis on the issue of privacy and personal information. The Insurance Act 18 of 2017 (IA) (2017) came into effect in South Africa on 1 July 2018. Section 12(4) of the IA prescribes that a controlling company must impose binding corporate rules on, or enter into a binding agreement with, every juristic person that is part of the insurance group, that includes terms regarding the processing of information, including personal information, within the insurance group. It can be argued that, in the absence of POPIA, the insurance industry could utilise personal information for direct marketing, as the main legislation governing the industry does not exert emphasis on deterring the use of personal information for unsolicited direct marketing by responsible parties.

4 PROPOSED PERSONAL INFORMATION PROCESSING MANAGEMENT FRAMEWORK (PIPMF)

In social contract theory application, an organisation collecting personal information can only be considered fair if the data subject is granted control over information and is informed about the organisation's intended use of the information (Malhotra et al., 2004). The conceptual personal information processing management framework (PIPMF) is proposed in figure 2 to aid in ensuring that procedural justice is achieved when processing personal information. The PIPMF was constructed using the following:

- Head and Yuan's theoretical framework for privacy protection in electronic commerce (2011);
- conditions of POPIA (2013); and
- The social contract theory of K. Martin (2016) and the framework of Malhotra et al. (2004);

The PIPMF includes elements from Head and Yuan's theoretical framework for privacy protection in electronic commerce (2011), which identifies key parties and their interaction in the privacy violation and protection context. The 4 main parties identified by Head and Yuan (2011) are: privacy subject (referred to as data subject in this study); information collector (referred to as the responsible party in this study); privacy violator (referred to in the model as 3rd party); and privacy protector. The identified parties interact with each other through interrelated activities, namely: collection activities; privacy violation activities; and privacy protection activities. The PIPMF adopted and added three actors to the framework, namely the responsible party (within the boundary), the data subject and third parties (outside the boundary). In their model, Head and Yuan were not explicit on the conditions that a responsible party must adhere to when collecting and processing personal information.

The PIPMF presented in this research includes the conditions of POPIA, namely: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, data subject participation and security safeguards that a responsible party must observe.

Interaction between the data subject, privacy subject, and responsible party are also adopted. Illegal information flow from the responsible party to a 3rd party is referred to as either *break-in* or *trade* depending on how the information is accessed (2011). If the responsible party voluntarily shares information illegally with a 3rd party, this is referred to as trade. On the other hand, if the 3rd party illegally accesses information directly from the responsible party's databases without their consent, this is referred to as break-in.

In addition, direct marketing and transborder data flows are also included. These conditions are depicted in the blocks in the framework within a processing boundary of the accountability of the responsible party.

Personal information of the data subject can be processed by the responsible party who must implement the conditions of POPIA, depicted by the personal information flow line A. This flow would include personal information which the data subject shares with the responsible party as well as direct marketing from the responsible party to the data subject. A responsible party can share personal information of the data subject with a third party (operator) provided the provisions in section 20 and 21 are complied with, which for example, include having a written contract in place between the two parties (illustrated by the flow of personal information in line B). However, the third party could also utilise these details to contact the data subject for direct marketing as illustrated by the flow of personal information in line C. The direct marketing must, however, be in compliance with the POPIA requirements.

In information privacy, a social contract is a mutually beneficial pact between parties in a community that dictates how personal information is utilised and shared (K. Martin, 2016). The social contract theory specifies that rules for customer information sharing should account for the purpose of data exchange, the risk involved and potential harm to the customer (K. D. Martin & Murphy, 2017). The approach adopted in this theoretical framework is centred on the social contract theory whereby consumers have certain expectations when they share their personal (Head & Yuan, 2011) information with organisations (Malhotra et al., 2004). Their initial position prior to the contracting is referred to as an initial state whereby they have certain expectations and secondly, where they have behavioural tendencies according to K. Martin (2016).

In the context of Figure 2 the initial state is observed in the data subject who has certain expectations about what personal information will be shared, with whom and how it will be used by the organisation or third party. The expectation for the processing of personal information in terms of who, what and how should be in line with the requirements of POPIA as a minimum requirement. As such the tenets of the social contract, as defined by K. Martin (2016), is considered in Figure 2. He refers to procedural contract norms whereby notice and choice is required for informed consent. This is embedded in the conditions of purpose specification (informing the data subject about “what” the purpose of collection or processing is), openness (informing the data subject about “who” is collecting the information and “how” it will be used) and further processing limitation (obtaining consent for sharing with third parties linking to “who” and “what”), which is usually reflected in an online notice or terms and conditions of websites.

Micro contract norms of social contracts focus on privacy as confidentiality and secrecy which are reflected in the security condition of POPIA. In such instances the contract must also follow procedural norms of consent and data subjects must be allowed to exit the contract which maps to the processing limitation condition of POPIA where the requirements for consent, justification and objection are included. Similarly, the tenet of chaining how information is used or the control thereof is addressed by the further processing limitation whereby consent would be required for alternative purposes to which the data subject did not originally consent under the purpose specification condition.

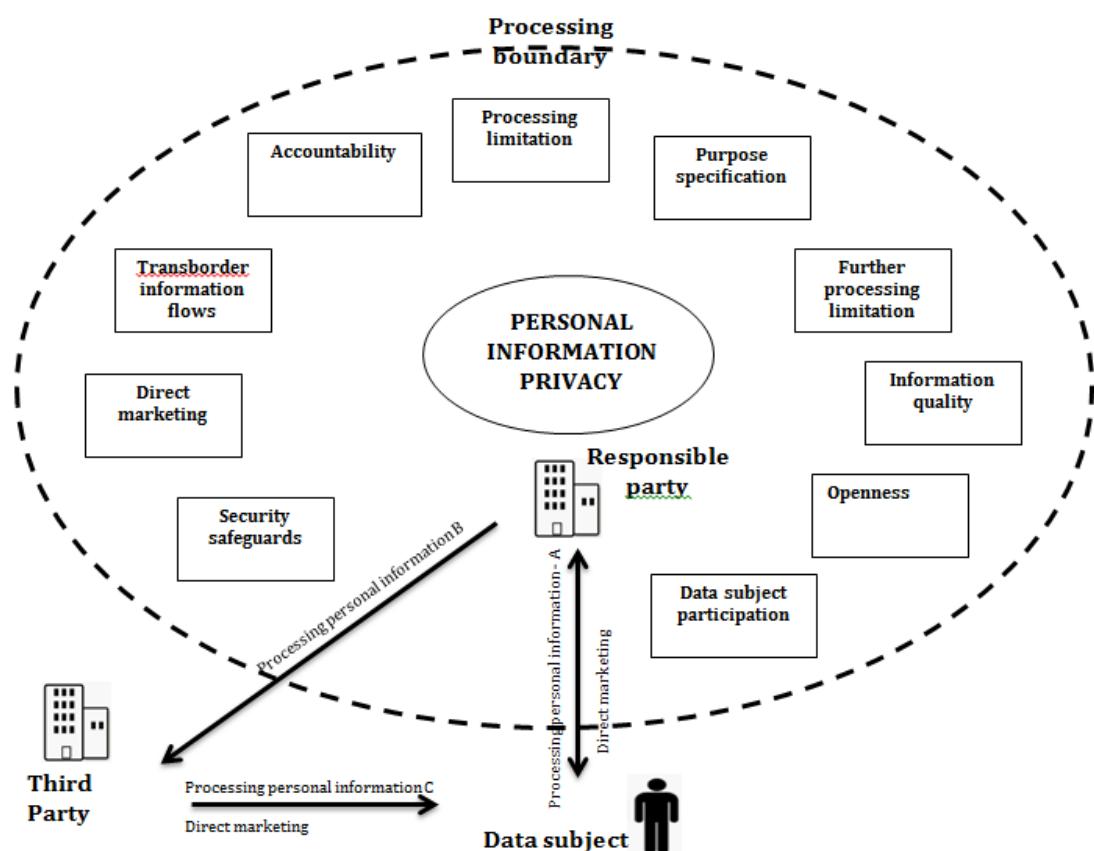


Figure 2: Personal information processing management framework (PIPMF)

The last tenet of Martin relates to the integrity of communities depicted as decisional privacy whereby legislative and substantive norms are considered. In this respect the POPIA conditions would serve as the minimum data privacy regulatory requirements applicable the social contract scenario depicted in Figure 2. The theoretical framework in Figure 2 indicates that data subjects share personal information willingly with responsible parties, with an agreement that information will be utilised only for the specified purpose thereby having a certain expectation of how their information will be processed and with whom it will be shared. According to the social contract depicted in the model, the responsible party is not allowed to create value chains by sharing customer information with third parties unless consent is obtained. These third parties are prohibited from approaching the customers with more than one instance of direct marketing unless they opt in thereby ensuring that the expectations of the data subject is met.

If all the conditions of POPIA are met, then privacy of personal information will be maintained as depicted in the centre of the framework with the personal information privacy oval.

The processing of personal information of line A, B and C will be monitored for compliance in this experiment.

5 RESEARCH METHODOLOGY

5.1 Paradigm

In this research, a positivism paradigm was utilised. A positivism paradigm states that reality is fixed and, therefore, knowledge that is objective can be generated through a rigorous research methodology (Broom & Willis, 2007). The positivism paradigm should utilise a quantitative research approach (Broom & Willis, 2007). The main philosophical aspects that are utilised to differentiate research paradigms are epistemology and ontology (Wahyuni, 2012). The epistemology philosophy for the positivism paradigm holds that credible facts and data can only be obtained for an observable phenomenon (Wahyuni, 2012). In this research, the observation of direct marketing communication, where consent has not been granted, is an observable phenomenon and thus the epistemology supports the use of the positivism paradigm. Ontology refers to the position that one has on the nature of reality. The positivist must be objective, external and independent of social factors.

In this research, the researcher will be objective and initially assume that companies comply with the requirements of POPIA. This ontology dimension further supports the use of the positivism paradigm.

5.2 Research design

To complement the positivism paradigm selected in this research, it is imperative to use a quantitative research approach. Experimental research was used in this research. The utilisation of experiments as a research method has a long history in information systems (Gupta,

2014). A profile is created by pairing a new cellphone to a new e-mail account. Six profiles were created and allocated to experiment and control groups. The experiment group received treatment or stimulus and the control group did not (Gray, 2013). This stimulus was applied to two profiles allocated to the experiment group; by using their e-mail address and contact numbers to request insurance quotations from 20 insurance companies online. The four profiles that were allocated to the control group were not used to source any online quotation. The personal information flow of data collected from both the experiment and control groups were monitored to establish the level of adherence to POPIA, and recorded. The researcher observed whether companies continued to send direct marketing communication after the subject had opted out from receiving marketing communication. Experimental research has an advantage in that it gives the researcher control over the variables and, in the process, eliminates external conditions that could confuse the results (Vargas, 2017).

5.3 Research strategy

In this experiment, the researcher deposited personal information on the websites of insurance companies, requesting online quotations. The researcher bought two new SIM cards and opened two new e-mail addresses. SIM cards A and B were matched with e-mail addresses A and B respectively. The combination of SIM card A and e-mail address A was used to apply for online quotations and opting in to receive marketing material. The combination of SIM card B and e-mail address B was used to apply for online quotations and opting out from receiving any marketing material. The online quotation requests were sent to 20 insurance companies. The details of the data deposited were recorded in an Excel workbook. The researcher portrayed himself as a 44-year-old male who lives in Pietermaritzburg, South Africa. This portrayal was utilised for profiles A and B. The e-mails were monitored twice a week and the cellphone communication was monitored during working hours. The details for communication received on the cellphones and e-mail addresses were recorded. Companies that were not part of the initial list were questioned on how they obtained the researcher's personal information.

The communication from the 20 insurance companies and others outside the initial group was monitored for compliance with POPIA for a duration of four months (May to August 2017). The following aspects were tested in this experiment in support of answering the main research question:

- Do all companies in the sample include an opt-in or opt-out preference for direct marketing on their websites when collecting personal information belonging to data subjects for the purpose of an online insurance quotation?
- How many communications did the data subject receive from the sample organisations where he or she respectively opted in and or out for direct marketing?
- Did companies that were not part of the sample contact the data subject? How many contacts were received from companies that were not part of the sample?

- Do all companies in the sample have a privacy disclaimer or policy on their website?
- Did all SMSs received include an opt-out preference, free of charge to the data subject?

5.4 Data analysis

Pivot tables were used in Microsoft Excel to derive statistical information (Gupta, 2014). A pivot table gives a way to efficiently summarise and display data in a spreadsheet by automatically displaying important selected statistical information, such as count, sum, standard deviation and others, based on a selected field (Moise et al., 2003). A total of 52 marketing communications was received comprising of SMSs, e-mails and cellphone calls.

6 FINDINGS AND DISCUSSIONS

In this section, the findings are highlighted and simultaneously discussed based on a synopsis of the research study in Table 2. The research questions are provided in the first column of Table 2; the proposed PIPMF framework monitored the data flow (represented by personal information flow A to C in the framework) in the second column; the results of the communications received back on the cellphone numbers and email addresses are portrayed in column 3 (evidence obtained); and the last column includes a description of the specific requirement of the applicable section of POPIA which companies need to comply with.

6.1 Inclusion of opt-in or opt-out on website

The personal information flow A of PIPMF relates to POPIA (2013), section 69(1a) that stipulates that the data subject must give consent for processing of data; section 69(2a) a responsible party may approach a potential customer only once to obtain marketing consent; and section 69(3c) a responsible party should give the data subject an opportunity to opt in for receiving marketing communication at the time when information is collected. The evidence obtained in testing this requirement of POPIA revealed that 75% of the companies did not have a facility on their website for data subjects to choose whether or not they opted to receive marketing communication when requesting online quotations. In addition, 5% of the companies sampled had a compulsory opt-in; such mandatory opt-in arrangement left the researcher with no option but to opt in. This mandatory opt-in creates an impression that the data subject has voluntarily agreed to receive marketing communication. Thus the majority of the companies in the sample did not provide their customers with any choice to opt in or to opt out from receiving marketing communication. Only 20% of the companies had a facility to opt out on their website.

This implies that 80% of the companies in the sample were not compliant with this aspect of POPIA.

Table 2: Synopsis of research study

Project aspect monitored for compliance	PIPMF data flow	Evidence obtained	Applicable section of POPIA legislation
6.1 Inclusion of opt-in or opt-out on website	Personal information flow A	75% provided no option to opt in or opt out on website 5% mandatory opt-in 20% provided opt-in and opt-out function on website	S69 (1)(a) The data subject has given consent. S69(2)(a) A responsible party may approach a potential customer only once to obtain marketing consent. POPIA S69(3c) A responsible party should give the data subject the opportunity to opt in or to opt out for receiving marketing information at information collection.
6.2 Direct marketing communications received from opt-in and opt-out	Personal information flow A	8% of all communications based on opt-in 46% received from companies where no option was provided at data collection 46% received by data subject from companies where the data subject opted out (in total 92% unsolicited) In addition, four companies (from opt-out) repeatedly contacted the data subject ignoring the POPIA requirements	S29(2) A responsible party may approach a potential customer only once to obtain marketing consent. POPIA S69(3c) A responsible party should give the data subject the opportunity to opt in or to opt out for receiving marketing information at information collection.
6.3 Third-party contacts received	Personal information flow B and C	2% (one company)	S69 (1)(a) Processing should only be carried out with consent, for contractual purposes, obligations imposed by law to protect legitimate interests, or for performance of public duty. S69(2)(a) New customers may only be contacted once and should opt in for further marketing.
6.4 Privacy disclaimer or privacy policy on website?	Personal information flow A	100%	S13(2) and S18(1) Customers must be informed of the reasons for data collection.
6.5 Opt-out preference in SMSs free of charge?	Personal information flow A and C	86% of SMSs pay to opt out 50% of messages did not contain the details of the company contacting the data subject	S69(3) A data subject must be afforded an option to object to receiving communication free of charge.

6.2 Direct marketing communications received from opt-in or opt-out

The PIPMF personal information flow A monitored the direct marketing communications received from opt-in and opt-out. It was found that 92% of the marketing communication received contained no prior agreement by the data subject to send direct marketing communication. The 92% also included instances where the researcher was not given any option to opt out (46%) at data collection as well as where the researcher opted out, but still received communication (46%). Section 69(2) of POPIA prescribes that a responsible party may approach potential customers to obtain their consent for marketing communication only once; thereafter, the responsible party may only contact customers that have opted in to receiving marketing communication. Contacting customers who have opted out from receiving marketing communication is prohibited by POPIA. However, four companies of the research sample communicated marketing-related messages more than once, in direct contravention of POPIA, section 69(2). Existing customers may be contacted for direct marketing where the direct marketing relates to similar products or services of the same responsible party, still including an opt-out provision.

6.3 Third-party contacts received

To determine if the data subject's information was shared with third parties, the personal data flow B and C in PIPMF was monitored. A single call was received from company 21, which was not part of the list of companies that were originally contacted for online quotations by the researcher. The communication from company 21 constitutes 2% of all the communication received. This contravenes section 69 of POPIA, which prohibits the sharing of a data subject's personal information without his or her consent. However, the communication from company 21 constitutes only 2% of all the communication received and therefore cannot be regarded as conclusive in respect of the prevalence of sharing of personal information by the South African insurance industry. The confession by the call centre agent from company 21 that information was obtained from a customer database points to the existence of sharing of data subjects' personal data with third parties by responsible parties.

6.4 Privacy disclaimer or privacy policy on website

It was encouraging to note that websites for all the companies in the sample had a privacy policy or disclaimer for customers sourcing online quotations. This assists customers to understand the reason why personal information is being collected from them, as prescribed by sections 13(2) and 18(1) of POPIA (monitored at data collection through personal information flow A in PIPMF). Despite the existence of a privacy policy in the sample, companies need to be measured on whether they adhere to their privacy policies or disclaimer. Section 6(1) of POPIA specifies that adequate measures must be put in place to prevent and detect organisations that do not adequately safeguard and respect personal information that they collect.

6.5 Opt-out preference in SMSs free of charge

Although all direct marketing SMSs received had a clause to allow the researcher to opt out of communication, 86% of the direct marketing SMSs required the data subject to pay for SMSs to opt out of any further marketing communication. Section 69(3c) of POPIA prescribes that the data subject must be afforded an option to object to receiving communication free of charge. This implies that the majority of the companies in the sample did not comply with POPIA by charging data subjects for SMSs when objecting to receiving direct marketing communication. Furthermore, 50% of the marketing SMS messages received did not contain details of the companies contacting the researchers; therefore preventing individuals from objecting to receiving direct marketing communication.

7 RECOMMENDATIONS

It is recommended that the Information Regulator should embark on a campaign to educate industries about non-compliance issues and the resultant implications. Specific champions can be identified in the different sectors, for example insurance, to compile guidelines on compliance within specific industries. The non-compliance that was displayed in this experiment can act as an early warning to the insurance industry to start directing its efforts towards complying with POPIA, before enforcement by the Information Regulator commences. The results are also a reflection of some of the challenges that the Information Regulator for POPIA faces in enforcing compliance by companies. This information can greatly assist other African countries that are still grappling with the implementation of information privacy regulations. The following are some specific aspects to concentrate on, as identified in this study:

- Online companies must include an opt-in and opt-out option for direct marketing on their websites at the point of collection of personal information.
- Companies that conduct direct marketing must include their contact information to allow potential customer to opt out from receiving marketing communication.
- Messages to unsubscribe from direct marketing must be free of charge.

8 LIMITATIONS AND FUTURE WORK

It is assumed in this research project that mobile phone operators will not re-issue or recycle mobile numbers, as mobile numbers previously utilised by any other person may compromise the research results. This is especially so in instances where the previous mobile number user contacted insurance companies for a quotation and opted in for marketing communication. It will have a negative impact on the results of the experiment if any of the cellphone numbers used was recycled. The experiment was conducted over a very short period, and as a result, the findings need to be verified by conducting the research over a longer period. At the time of the

experiment POPIA had not commenced as yet and as such some companies in the sample may still be in the processes of implementing the requirements of POPIA. It is therefore suggested to repeat the study in the form of a comparative study once POPIA commences.

9 CONCLUSION

The purpose of this research was to establish whether insurance companies adhere to the direct marketing provisions of POPIA when processing personal information. The personal information processing management framework was proposed and depicts the conditions of POPIA as well as the flow of personal information between different actors included in the scope of this study. In this experiment, it emerged that 92% of the marketing communication received had no prior consent from the data subject, indicating a violation of this specific POPIA provision. Although online quotations were requested from insurance companies, the data subject did not consider himself a customer due to his non-acceptance of the quotations. Some companies that were not given personal information by the researcher also contacted the researcher trying to sell goods and services. It was evident that companies are contacting data subjects with marketing material without seeking prior consent. Traces of sharing of data subjects' personal information with third parties was evident as the researcher was contacted by companies that were never given personal and contact information by the researcher. Furthermore, 86% of these companies required customers to pay for SMS messages requesting to be excluded, and half of the marketing SMS messages received did not contain details of the companies contacting the researchers, therefore preventing individuals from objecting to direct marketing. This indicates that some insurance companies in South Africa are not compliant with POPIA conditions. This research has indicated that companies are violating the requirements of the direct marketing of POPIA by contacting data subjects even if they did not opt in, and by sharing their personal information with third parties.

References

Abdulrauf, L. A., & Fombad, C. M. (2016). The African Union's data protection convention 2014: A possible cause for celebration of human rights in Africa? *Journal of Media Law*, 8(1), 67–97. <https://doi.org/10.1080/17577632.2016.1183283>

African Union. (2014). African Union convention on cyber security and personal data protection [Last accessed 18 Jul 2020]. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Akhter, S. (2014). Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*, 31(2), 112–125. <https://doi.org/10.1108/JCM-06-2013-0606>

Baloyi, N., & Kotze, P. (2017). Are organisations in south africa ready to comply with personal data protection or privacy legislation and regulations?, In *2017 IST-Africa Week Conference (IST-Africa)*. <https://doi.org/10.23919/ISTAFRICA.2017.8102340>

Borena, B., Belanger, F., & Egigu, D. (2015). Information privacy protection practices in Africa: A review through the lens of critical social theory, In *48th Hawaii International Conference on System Sciences (HICSS)*. <https://doi.org/10.1109/HICSS.2015.420>

Botha, J., Grobler, M. M., Hahn, J., & Eloff, M. (2017). A high-level comparison between the South African Protection of Personal Information Act and international data protection laws, In *ICMLG2017 5th International Conference on Management Leadership and Governance*.

Broom, A., & Willis, E. (2007). Competing paradigms and health research, In *Research Health: Qualitative, Quantitative and Mixed Methods*.

Curry, E. (2016). The big data value chain: Definitions, concepts, and theoretical approaches, In *New horizons for a data-driven economy*. Springer. https://doi.org/10.1007/978-3-319-21569-3_3

de Bruyn, M. (2014). The Protection of Personal Information (POPI) Act–Impact on South Africa. *International Business and Economics Research Journal*, 13(6), 1315–1340. <https://doi.org/10.19030/iber.v13i6.8922>

European Commission. (2013). A European strategy on the data value chain [Last accessed 21 Jun 2020]. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=3488

European Union. (2016). General Data Protection Regulations 2016/679 of the European Parliament and of the Council of 27th April 2016 (GDPR) [Last accessed: 18 Jul 2020]. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Gray, D. E. (2013). *Doing research in the real world*. Sage.

Greenleaf, G. (2017). Countries with data privacy laws–By year 1973-2016 [Last accessed 18 Jul 2020]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2996139

Grobler, M. M., Eloff, M., & Hahn, J. (2015). Evaluation of online resources on the implementation of the Protection of Personal Information act in South Africa, In *10th International Conference on Cyber Warfare and Security: ICCWS 2015*.

Gupta, S. (2014). SEM for experimental designs: An information systems example. *Electronic Journal of Business Research Methods*, 12(1), 27–40.

Hartemo, M. (2016). Email marketing in the era of the empowered consumer. *Journal of Research in Interactive Marketing*, 10(3), 212–230. <https://doi.org/10.1108/JRIM-06-2015-0040>

Head, M., & Yuan, Y. (2011). Privacy protection in electronic commerce–A theoretical framework. *Human Systems Management*, 20(2), 149–160.

Krafft, M., Arden, C. M., & Verhoeff, P. C. (2017). Permission marketing and privacy concerns. *Journal of Interactive Marketing*, 39, 39–54. <https://doi.org/10.1016/j.intmar.2017.03.001>

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, 137(2), 551–569. <https://doi.org/10.1007/s10551-015-2565-9>

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/10.1007/s11747-016-0495-4>

Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current Opinion in Psychology*, 31(1), 116–121. <https://doi.org/10.1016/j.copsyc.2019.08.010>

Moise, W. P., Conlon, T. P., & Thompson, M. L. (2003). Automatic formatting of pivot table reports with a spreadsheet [US Patent 6,626,959].

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2011). *Security in computing* (5th). Prentice Hall.

RSA Government. (1996). Constitution of the Republic of South Africa [Last accessed 18 Jul 2020]. <https://www.justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf>

RSA Government. (1998a). Long Term Insurance Act [Last accessed 18 Jul 2020]. <https://www.gov.za/documents/long-term-insurance-act>

RSA Government. (1998b). Short Term Insurance Act [Last accessed 18 Jul 2020]. <https://www.gov.za/documents/short-term-insurance-act>

RSA Government. (2009). Consumer Protection Act [Last accessed 18 Jul 2020]. <https://www.gov.za/documents/consumer-protection-act>

RSA Government. (2013). Protection of personal information act [Last accessed 18 Jul 2020]. <https://www.gov.za/documents/protection-personal-information-act>

RSA Government. (2017). Insurance Act [Last accessed 18 Jul 2020]. <https://www.gov.za/documents/insurance-act-18-2017-english-afrikaans-18-jan-2018-0000>

Skolmen, D. E., & Gerber, M. (2015). Protection of personal information in South African cloud computing environment: A framework for cloud computing adoption, In *Information Security for South Africa*. <https://doi.org/10.1109/ISSA.2015.7335049>

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016. <https://doi.org/10.2307/41409970>

Spiekermann, S., Acquisti, A., Bohme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, 25(2), 161–167. <https://doi.org/10.1007/s12525-015-0191-0>

UK Government. (1998). Data Protection Act (UK) [Last accessed 18 Jul 2020]. <http://www.legislation.gov.uk/ukpga/1998/29/contents>

Vargas, P. T. (2017). A practical guide to experimental advertising research. *Journal of Advertising*, 46(1), 101–114. <https://doi.org/10.1080/00913367.2017.1281779>

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research, Winter*, 69–80.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behaviour*, 28(3), 889–897. <https://doi.org/10.1016/j.chb.2011.12.008>

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798. <https://doi.org/10.17705/1jais.00281>