PoPI Act - opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment

Paulus Swartz
School of Computing
University of South Africa
South Africa
paulus.swartz@absa.co.za

Adéle Da Veiga
School of Computing
University of South Africa
South Africa
dveiga@unisa.ac.za

***Abstract*—Personal information is collected and processed by various companies when individuals buy products and services, share their information on social media or enter their details in competitions and so on. This personal information, which could potentially also be shared with third party companies, is analyzed to tailor services and products to consumer's preferences and online behavior, with the objective of creating a data value chain. When the Protection of Personal Information (PoPI) Act (2013) comes into effect in South Africa, companies will have to comply with the conditions of PoPI and protect individuals' personal information accordingly. Companies will only be allowed to use personal information for the agreed purpose it was collected for and must obtain individuals' consent to share or further process their information.**

This research sets out to monitor the flow of personal information through an experiment to establish if data value chains are shaped within the South African insurance industry, and to establish whether the consumer's personal information, which is part of the data value chain, is processed in line with certain conditions of PoPI.

The experiment highlighted that some of the insurance companies in the selected sample did not comply with the opt-in or opt-out preferences of the researcher. In addition some did not meet with the condition to obtain consent before sharing personal information with third parties for marketing purposes. No formal data value chains could be identified during the time frame of this experiment as it was found that the researcher was contacted randomly about generic marketing and communication offerings.

Keywords—Protection of Personal Information Act; PoPI; data value chain; direct marketing; opt-in; opt-out; personal information; privacy; experiment

I. INTRODUCTION

Privacy is not a new concept. It is the right of the individual to be free from secret observation and to determine with whom, how and whether or not to share personal information [1]. For most people "privacy" is a meaningful and valuable thing, but the term has different meanings in different contexts [2]. Privacy is an essential component of individual freedom, civil liberties, autonomy and dignity [3, 4]. The right to privacy is the right to an individual's autonomy and personality, which is the individual's general right to immunity [3].

Individuals have a reasonable privacy expectation that companies, like telephone or internet providers, banks, government, medical practitioners and insurance companies would secure their personal information [3]. However, the right to privacy in the digital world is under attack as tracking surveillance is increasing and individuals' personal records are becoming more vulnerable while being stored digitally [3]. Contextual integrity is destroyed by selling or reusing digital information; even if users give their consent, they are not always aware of the purpose for which their information is later used [5]. Mismanagement of personal information processing, storage, use, collection and exchange can violate human rights. This could result in people losing trust in organisations, especially if the information is not secured and processed in accordance with regulatory requirements [6].

In South Africa the Protection of Personal Information Act (PoPI) (2013) was promulgated in November 2013 [7, 8]. This Act regulates the processing of personal information by public and private organisations domiciled in South Africa. PoPI includes a condition relating to unsolicited marketing, namely that consent is required in certain circumstances when existing or new customers are contacted. Organisations must comply with the conditions of PoPI and may only contact individuals in line with those conditions.

This research paper discusses research carried out to determine if customers' opt-out and opt-in preferences are honoured in the flow of personal information in the insurance industry, as required by PoPI. This research project forms part of a larger research project that honours students from the School of Computing at the University of South Africa participate in as part of their B.Sc. Honours degree.

The remainder of the research paper is structured as follows: Section II presents the research problem. This is followed by section III, which gives an overview of PoPI. Section V discusses the research methodology and section VI contains the results of the experiment. A discussion of the results and

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

limitations is presented in section VII, followed by the conclusion in section VIII.

II. Research Questions

The personal information processed by the insurance industry could be used to analyse individual preferences and to obtain competitive advantage with the aid of data value chains. These data value chains help organisations to make more effective strategic and operational decisions by directing services to specific customers or market segments [9]. However, data value chains could also pose a risk to the confidentiality and privacy of the information being shared with potential third parties or when used for purposes not agreed with the data subject (the person whose information it is).

Section 69 of PoPI prohibits unsolicited marketing unless the customer (data subject) consents to it. This means that new customers must opt-in for electronic communication, for example via cell phone text messages or e-mails. New customers may be contacted only once in order to obtain their consent (or opt-in) for marketing purposes.

Although it is thought that organisations have started the process of implementing the conditions of PoPI, many might not have. Once the provisons of PoPI come into effect, organisations will have one year to comply with the Act. Research [2] shows that only 12% of small and medium enterprises (SMEs) are in the process of complying, while 16% believe they are compliant, 56% are not aware of the conditions of PoPI and 16% are not compliant. Many organisations believe that it will require significant effort to become PoPI compliant, with some estimating that it could take in excess of 9 000 hours [10]. While some organisations have started with the implementation process, research indicates that it could take more than a year to become compliant, while many organisations believe that it could take up to three to five years to become compliant [30].

The following two research questions have therefore been formulated:

- What personal data value chains are there in the insurance industry in South Africa for the flow of personal information?
- Do South African insurance companies only contact customers if they have opted in for marketing and communication purposes as required by PoPI?

The answers to these research questions can indicate to organisations whether they comply with certain conditions for marketing in PoPI, and whether they are using clients' personal information to offer value services in the context of a value chain.

III. An overview of privacy legislation

A. International Privacy Regulation

Data protection laws have been adopted by over 100 countries and others are in the process of adopting privacy laws [8, 11]. The EU's Data Directive 95/48/EC is one of the best-known privacy laws [12]; [13] and it has recently been updated to the General Data Protection Regulation (GDPR) [14]. The GDPR addresses new technological developments and harmonises national data protection laws across the EU member states [15].

According to the parliament text of the proposed GDPR, consent must be explicit and indicate affirmative agreement from the data subject, and is valid as long as personal information is processed for the purpose it has been collected for. Reference [12], argue that the objective of privacy legislation is to enable the individual to (i) manage or control the flow of personal information and (ii) to give the individual autonomous space.

Owing to the growth of modern computing, data protection laws have been implemented in many countries. In 1974 the United States of America drafted their privacy legislation. Germany followed in 1977 and France in 1978 [12]. South African citizens' personal information is also processed outside South Africa by multinational organisations and through the internet, which renders the information vulnerable [6]. The sensitivity of personal information changes as it flows through the economy, therefore the security and privacy requirements are dynamic [16] and should at all times be processed in line with the regulatory requirements of the relevant jurisdictions.

B. Protection of Personal Information Act (PoPI), 2013

The purpose of PoPI is to provide a constitutional right to privacy by protecting the individual's personal information when processed by a responsible party. In this context the individual is referred to as a data subject, who is the "person to whom personal information relates" and who is an identifiable, living, natural or juristic person [17]. The responsible party is the, "public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information" [17].

Personal information is information relating to the data subject, such as biographical information (e.g. race, gender, marital status, disability or religion), education, medical or financial information, e-mail and physical addresses, biometric information, and even information about personal opinions and views, including correspondence [17].

PoPI regulates the manner in which personal information may be processed, in line with international standards and established conditions, according to the prescription of the minimum threshold requirements for the lawful processing of personal information.

PoPI also provides for the rights of data subjects and remedies available to them, to protect their personal information from processing that is not in accordance with the Act. PoPI provides for the establishment of an information regulatory body with certain duties and powers in line with the conditions of PoPI and the Promotion of Access to Information Act (PAIA), 2000 [18]. Funds for the

Office of the Information Regulator have been approved by the Minister of Justice and Treasury [19] in support of the implementation of the sections relating to the Information Regulator.

PoPI has a significant impact on an organisation's policies, employees, information technology infrastructure, third party service providers and procedures if the organisation aims to comply with the provisions of the Act [20]. It impacts responsible parties that collect, process and store the personal information of customers, employees and third parties as part of their operational activities [7]. The next section gives some insight into the perceived positive and negative impacts of PoPI.

C. Positive impact of PoPI

PoPI will have a positive impact from an organisational and data subject perspective.

Preventive Measures: Responsible parties who collect personal information must be accountable and transparent, and should safeguard personal information according to condition 7 of PoPI [34]. According to [7], companies are now implementing proactive technical and organisational measures in the hope that these will prevent the leaking of personal information . These measures should ensure that companies' databases are secure to prevent data leakage and to protect their investments.

Transparency: Another advantage, according to reference[7], is that companies will be more transparent in terms of how, what and where personal information is stored within the company. Companies must notify data subjects when personal information is processed (section 18, [17]), and data subjects have the right to opt-in or out, free of charge, to receive marketing communication (section 69, [17]). Consent must be given before personal information is shared with third parties for marketing purpose (sections 11 and 20, [17]), therefore data subjects should not under normal circumstances receive unsolicited text messages or phone calls [7]. All businesses or parties responsible for big data and the analyses of an individual's habits, purchase behaviours or health status must treat the information as if it has been collected by means of questionnaires [21]. They must therefore be transparent in their use of the personal information, ultimately protecting the right of the individual while abiding by ethical principles.

Individuals' Rights: If data are inaccurate, misleading, excessive or incomplete, or if data have been obtained unlawfully, data subjects can rightfully request an update, deletion or correction of their personal information according to section 16 of PoPI [22]. Reference [21] argues that the laws protecting the privacy of personal data give individuals rights to all their data, irrespective of the source. PoPI also enables individuals to institute civil proceedings under certain circumstances if there has been interference with the protection of their personal information (sections 5 and 99 of [17]).

D. Negative Impact of PoPI

Many organisations believe that PoPI will have a negative impact on them.

Marketing Costs: The Consumer Protection Act [23] of South Africa only allows for an opt-out mechanism. Section 11(5) of the Consumer Protection Act, 2008, states that if a consumer opt-out to receive direct marketing, no person must charge the consumer a fee to effect it. PoPI stipulates that affirmative consent is required, which means that individuals have to opt-in to receive direct marketing messages (section 69, [17]). PoPI also requires that the customer be given reasonable time to object, at no cost to the data subject, which means that the business is responsible for all costs when the customer opts out at a later stage [24]. Companies must update their IT systems to flag the option to opt-in or opt-out of direct marketing (section 11, [17]). Company processes for responsible parties and third parties must also be updated according to section 13 of PoPI, with provision that personal information can only be shared if the purpose is specific, the quality of information is ensured (section 16, [17]) and the information is safeguarded (section 19, [17]). This has an impact on the system design and administration process, on contracts with third parties.

Infrastructure Cost to Company: Critics have warned that the PoPI regulatory scheme will discourage economic activity and put undue burdens on businesses [25], because many businesses will have to make supplementary investments in information technology systems or use third-parties vendors in order to comply with PoPI.

Compliance Time Frames: To be compliant within one year is impracticable, as shown by a survey conducted by South African businesses in 2013. It could take up to three years to become fully compliant [10, 25]. Organisations have to overcome huge challenges to become compliant. Companies that are already implementing measures to comply with PoPI requirements are concerned that they will not be compliant in time [10]. A study done by Cibecs in 2012 shows that 26% of South African companies are in the process of complying with the requirements of the PoPI Act, and are therefore upgrading their IT infrastructure measures [26]. Research [26] indicates that as many as 38% of the companies surveyed still have outdated compliance measures in place.

E. Data Value Chains

A data value chain is the management and coordination of data across the service continuum, where a collaborative partnership is formed, and where data collection is coordinated from various stakeholders while analysing the data to optimise service delivery and product development [27]. Data that is generated by companies facilitates re-use and value generation based on the data, over and over again [28]. The European Commission states that the data value chain is the, "centre of the future knowledge economy, bringing the opportunities of the digital developments to the more traditional sectors (e.g. transport, financial services, health, and manufacturing)" [28].

Personal information can be utilised in data value chains to provide an improved service offering through focussed marketing, which can allow organisations to channel identified services to specific customers. However, customers must willingly share their personal information and organisations must only use it in line with the consented preferences of the customers.

F. Use of Personal Information for marketing purposes

Direct marketing entails that the marketer communicates directly with a customer or client in the hope that the customer will respond positively to the marketer's request [29]. Any type of electronic communication, like a text message (SMS) or a video message (MMS) to a mobile telephone, e-mails, mobile device application advertising and social media marketing, is a tool used by the marketer to advertise a service or products. Section 11 of the Consumer Protection Act (CPA) 68 of 2008 stipulates that every person has the right to privacy and to refuse to accept any approach or communication if the purpose is for direct marketing. According section 69 of PoPI, the processing of personal information for the purpose of direct marketing is prohibited, unless the marketer has the consent of the data subject, is a customer of the responsible party, the responsible party has the customer's contact details and they market similar products or services of the responsible party to the data subject.

Subsection 4 of section 69 of [17] states that the identity and address or contact details of the sender must be known to enable the recipient to respond to the request if they wish to do so. Consumer preference information is used by direct marketers to combine groups of consumers with the same interest and taste, and this information is beneficial for businesses as well as for the consumer to receive communication messages according to their personal preferences [30], which relate to a data value chain.

According to section 69 of PoPI, the customer must grant permission for the processing of personal information and must also have the option to cease any communications. The consent option for processing personal information is refered to as "opt-in", and the rejection of future communications from the marketer is referred to as the "opt-out" option. Consumers are sometimes misled about their choice to opt-in or opt-out on the company's websites or application forms. For example, the default setting on most websites is to opt-out, or the questions that are asked ("Please send me newsletters" or "Please do not send me newsletters") are trivial and might influence consumer decisions [31]. Because of inattention, and cognitive and physical laziness, default answers are given. Often the opt-in option is ticked by default [32].Marketers tend to set the "yes" option as default if they need the consumers to opt-in for the processing of personal information [32]. As such compliance with PoPI could impact negatively on organisations' freedom to use marketing and communication initatives.

IV. THE INSURANCE INDUSTRY

To be competitive in the insurance industry, companies have to market their products. Cold-calling is a method used by insurance companies to market their products, and according to [33], the Financial Advisory and Intermediary Services Act (FIAS) 37 of 2002 [34] and CPA address the issue, but it is PoPI that will eliminate the cold-calling sales technique. According to a study done in the health services, 6% of data breaches are committed by insurance companies, the third highest out of 17 industries [35]. Cybersecurity insurance is expanding rapidly in the insurance market, with a forecast of $7.5 billion in annual sales globally by 2020 by the global cyber insurance market [36, 37]. If an insurance company wants to provide cybersecurity insurance in South Africa, it must set an example and comply fully with the requirements of PoPI. The research reported in this paper has focused on the insurance industry, because it processes large quantities of personal information. The research results can provide the insurance industry with insight into possible gaps in compliance with PoPI.

V. RESEARCH METHODOLOGY

This section outlines the research methodology.

1)Positivism Paradigm

The positivism paradigm applies to this research. A postivism paradigm is based on realist ontology beliefs, where there is an object reality according to representational epistemology where symbols are used to explain and describe this objective reality accurately [38, 39]. Reference [39] states that positivism can reveal the causal relationship that exists within social life, such as the flow and use of personal information in the economy.

2)Experimental Design

An experimental design was used for this research project. This design allowed the researcher to have full control over the experiment and strengthens the internal validity [40]. Reference [41] suggest that if the experiment is carried out correctly, the testing effect, mortality, history and maturation, as possible pitfalls of internal validity, will not have an effect on the research outcome. Nevertheless, these pitfalls were avoided. Two groups were involved in the research, namely the experiment group and the control group; a stimulus was applied to the experiment group and no stimulus was applied to the control group [41].

3)Sample

This research focused on the insurance industry in South Africa. The insurance industry collects personal information through online applications, telephonic marketing, hard copy applications and also their claim process.

The geographical area was limited to South Africa. The head offices of the insurance companies included in the sample are mainly located in the metropolitan cities of each province.

Twenty insurance companies were included in the sample. The sampling method used for this research project was a convenience sample [36]. A prerequisite for inclusion in the sampling was that the insurance company had to have a website where online insurance applications could be requested.

B. Research Design

1)Experiment Preparation

To conduct the experiment, two new cell phone numbers and six new e-mail addresses were utilised, which allowed the researcher to supply his personal information when requesting online quotations from the sample of insurance companies.

Once the reseacher had requested quotes from an insurance company via its website, the researcher's personal information, including a cell phone number and/or e-mail address, was requested and processed by the insurance company. The information was therefore included in the customer records in the companies' databases. In this way the researcher's personal information was deposited in the economy, and the researcher was able to monitor the flow of his personal information (each new cell phone number and e-mail address). The researcher used an identical profile in his dealings with all the insurance companies selected for the research. While the research project was undertaken, the cell phone numbers and e-mail accounts were not used for any other purpose.

Table 1 shows the two new cell phone numbers, Cell phone A and Cell phone B, which were created in March 2015 for the purpose of this research. When the researcher purchased sim cards from the service provider, his information was verified in line with the Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act, 2002 [43].

Company Name	Cell phone A / E-mail A	Cell phone B / E-mail B
Company A - J	Opt-In	Opt-Out

Table 1: Group 1 Companies

The six e-mail accounts were created in April 2015. Two of the six e-mail addresses were linked with the cell phone numbers in Table 1. The cell phone numbers and related e-mail addresses were disclosed to the first ten insurance companies (see Table 1). This experiment was conducted from a consumer perspective and hence to protect the confidentiality of the companies in the sample their names are withheld.

The remaining four e-mail addresses (see Table 2) were included in the personal information supplied to the next ten insurance companies in the sample. Combination of two email addresses was used in group 2 for opt-in and opt-out to determine the data value chains that will be created without the cellphone numbers linked to the email addresses. It was found that no information could be submitted without a cell phone number. Cell phone A was therefore also submitted with e-mail addresses C and D, and cell phone B was submitted with e-mail addresses E and F.

Company	Cell phone A / E-mail C	Cell phone A / E-mail D	Cell phone B /E-mail E	Cell phone B / E-mail F
Company K – T	Opt-In	Opt-In	Opt-Out	Opt-Out

Table 2: Group 2 Companies

In order to monitor whether the opt-in and opt-out preferences were maintained, the researcher opted in for all communication when requesting online quotations using cell phone number A, and opted out for all online quotations using cell phone number B.

For the control group, the researchers purchased four cell phone sim cards. The researchers activated the numbers on the network by sending at least one SMS to another number. No stimuli were applied to these numbers, meaning that the researcher did not disclose the cell phone numbers to any company nor use it for phone calls or text messaging. This would eliminate any biased results during the experiment, because the cell phone numbers were not subjected to any experimental treatment.

2)Conducting the Experiment

Personal information was disclosed to the insurance market in May 2015. The method used to disclose personal information was to request life insurance or short-term policy quotations from insurance companies using the online application tools on the companies' websites.

3)Data Collection

Data were collected by means of telephone calls, SMSs and e-mail messages received from companies that contacted the researcher on either of the two cell phone numbers or any of the six e-mail addresses created for this experiment. Information about each telephone call and SMS was recorded daily on a spreadsheet, and information about e-mail messages received was recorded twice per week.

The time frame for collection was restricted to the period March to October 2015 to accommodate students enrolled for the one-year Unisa honours degree module.

During this time the researcher recorded certain aspects, such as the origin of contact details; whether the researcher opted in for the communication; whether there was an option to opt-out of any future communication; whether the researcher was liable for any cost when opting out; and whether the researcher was contacted by an automated telephone. Questions such as "Where did you get my contact details?" and "Do you have my name and surname?" were asked to

telemarketers or call centre callers who telephoned the researcher. This provided the researcher with an indication of whether the researcher was known to the company and whether calls were made to random numbers. It also helped the researcher to establish whether they obtained his personal information as a result of the online insurance application process.

4)Findings

Table 3 outlines a summary per company of the number of times the researcher where contacted where the opt-in or opt-out preference was selected. In total the researcher was contacted 84 times during the data collection period of which 47 contacts were linked to the companies included in the sample and 37 were related to companies who contacted the researcher were not part of the sample 55% of all communications were received via SMSs and 28% via e-mail messages. Telephone calls only accounted for 17% of his contact with direct marketers. The 28% e-mail messages that were received were generated when quotations had been requested from insurance companies.

Thirty percent of the total communications received (84) related to contacts where the customer opted in for communication by the insurance companies. For 70% of the contacts the researcher had not opted in for communications by entities indicating that the opt-out preference had not been complied with.

Company Name	Opt – In Number of contacts	Opt-Out Number of Contacts
Company A	1	3
Company B	0	0
Company C	0	1
Company D	1	1
Company E	1	1
Company F	1	0
Company G	2	0
Company H	0	0
Company I	1	0
Company J	2	0
Company K	1	8
Company L	0	0
Company M	2	0
Company N	2	0
Company O	6	6
Company P	3	0
Company Q	2	0
Company R	0	0
Company S	2	0
Company T	0	0
Total	27	20

Table 3: Number of contacts received per company for opt-in and opt-outs

Phone calls were received from the insurance companies who called about the quotations requested. Only 22% (10 out of 46) SMSs sent by the insurance companies had the researcher's personal information; 18% were sent by the cell phone service provider.

The remaining 60% of SMSs received came from entities who had no permission to contact the researcher and who had no information about the researcher.

Where the researcher opted out for marketing communications, 20 communications were received. Of these, 30% were received from cell phone B combined with e-mail B, which indicated non-compliance with the opt-out reference.

The other 70% were received from cell phone B combined with e-mails E and F. Similarly, where the researcher opted in for future communications, a total of 27 communications were received of which 33% were from e-mail A linked to cell phone A and 67% were from e-mails C and D.

Interestingly, in 37 of the instances the researcher was contacted by 18 different companies who were not part of the sample. This indicated that the information could have been shared with third parties who used it to contact the researcher.

These companies did not have permission to contact the researcher for marketing purposes via the cell phone numbers and e-mail addresses used in the research. Most of these companies only contacted the researcher once, but 2 companies contacted the researcher at least 8 times each during the experiment to offer financial services or to notify him that he had won a competition.

On cell phone B, where the researcher opted out for communication, the researcher received 9 calls, seven SMSs and four e-mail messages. The researcher received 5 calls, two SMSs and 20 e-mail messages on the cell phone number where opt-in was elected for communication.

The results indicate that half (six out of 12) of the contacts made by Company "O" were permitted and used e-mail address C or D. There was no consent for the other half of the communications received from Company "O", as the researcher had opted out when using e-mail addresses E and F. There was no consent for 90% (8 out of 9) of contacts made by Company "K" – there was a privacy disclaimer on the website regarding the protection of personal information that said the researcher would only be contacted about a requested quotation.

Company "A" contacted the researcher 4 times. This company also had a privacy disclaimer on their website, indicating that they would protect the researcher's personal information and would only contact the client about a quotation requested. The researcher elected to opt-out of communication from Company "A", but no option was provided to opt-out during the application process. The websites of Company A and Company K did not offer opt-in or opt-out options on their application/quotation systems, but they did include privacy

disclaimers that promised to protect the customer's personal information.

38% of the entities that contacted the researcher did not have the researcher's personal details, and it was unknown how the researcher's contact details had been obtained for 35% of the communications received.

Only 43% of the SMSs received included the option to opt-out of communications. Most of the 43% of the SMSs that included the option to opt-out, indicated that standard rates would apply to opt-out. None of the phone calls received were from an automated calling machine.

The control group received a total of 70 communications, 9 missed calls and 61 SMSs. Three of the cell phone numbers (Cell Phone Provider I; Cell Phone Provider II; and Cell Phone Provider III) did not receive any communication except SMSs from organisations. Cell Phone Provider IV accounted for 9 missed calls, of which six were from different numbers, as well as six SMSs. These SMSs were messages from financial service providers or a message that a competition had been won. This cell phone number might have been owned and used by another individual in the past, which could explain these messages. This can be further investigated to determine the source, why the cellphone number is link to a marketing database.

VI. Discussion

The researcher had only given consent for 33% of the 84 communications received (e-mail messages, SMSs and telephone calls). The opt-out group received more calls and sms's (9 calls, 7 sms's) than the opt-in group (5 calls, 2sms's), during the research. Seventy six per cent of the entities had not obtained the researcher's consent to contact him. Section 69(1) of PoPI stipulates that data subjects must give their consent to the responsible party to process their personal information and must opt-in for marketing purposes. 42% of the responsible parties did not have any consent to contact the researcher for marketing purposes. In addition, Companies 1 to 18 were not even part of the sample. This answers research question 2, indicating that customers are contacted even though they have not opted in for marketing and communication purposes as required by PoPI.

This indicates that insurance companies might not be fully compliant as yet, as some do not have the proper consent options (opt-in/opt-out mechanism) for the client (data subject) or do not abide by it, while others have disclaimers on their websites, but do not abide by them.

At the time when the data were submitted via the insurance companies' websites, only five out of 20 companies made provision for clients to opt-in or opt-out for any marketing communications. In future, organisations will have to give new customers the option to opt-in for marketing and communication, and allow existing customers to opt-out at any time for marketing and communication purposes, as per section 69 of PoPI.

There were 2 companies that included a privacy disclaimer on their websites, stating that they valued the researcher's personal information, would protect it and would only contact the researcher about the product or service he is interested in. However, these companies did not comply with section 69 of PoPI, which states that a data subject must give his/her consent for the processing of personal information for marketing purposes.

Almost half of the SMSs received were sent by entities that did not give the researcher the option to opt-out of direct marketing communications. This means that the responsible persons or third party did not comply with the regulations of PoPI. Data subjects must be given the option to opt-out of or withdraw their consent for the processing of information and future marketing communications from third parties as per section 69(4b) of PoPI.

Direct marketing from the companies that were not part of the sample did not comply with PoPI regulations, as these companies contacted the researcher via SMS for marketing purposes without consent to do so.

The third party or organisation responsible for direct marketing must supply its address or contact details as per section 69(4b) of PoPI, to enable recipients to opt-out of any future communication. 43% of the companies that sent SMSs without an opt-out option did not comply with PoPI. Section 69(3) of PoPI, states that the customer must have the option to consent or cease communication at free will, at any future marketing communications.

Because SMSs were received from unknown senders as well as organisations who were not included in the sample, it was difficult to establish the origin of all messages or how personal information was leaked or shared to these entities, because the researcher was in no position to confirm how the entity got the information to make contact with the researcher. However, these messages indicated that data, specifically personal information, were shared in the economy with third parties as the cell phone numbers and e-mail addresses were only used when submitting the information on websites of insurance companies included in the sample.

In conclusion, it was found that at the time of the research there were no significant personal data value chains created by the insurance industry in South Africa for the flow of personal information, which answered research question 1. The researcher was contacted randomly and not for products or services tailored to his demographic profile. It was also concluded that the researcher had been contacted by companies that had no consent, which answered research question 2.

VII. Limitations

For the purpose of the experiment it was assumed that companies were in the process of becoming compliant with

PoPI as it has been promulgated for three years now and companies will only have one year to become compliant once in effect. A limitation was that the conditions of PoPI, apart from those relating to the establishment of the Information Regulator, were not yet enforced, which means that companies do not have to be compliant as yet unless they are a multinational organisation operating in other jurisdictions with data protection laws. This could be why the results of the research indicated non-compliance for certain sections and conditions of PoPI. Taking into consideration that it could take between three to five years to become compliant it is anticipated that companies should have started to implement measures to prepare for compliance.

Another limitation of the research project was the limited time frame available to monitor communication to the cell phones and e-mail addresses created. This could not be avoided, because the honours project had to be concluded within a year.

A further limitation was that some cell phone numbers had previously belonged to other people, therefore some of the communications received via sms during the research might have been meant for the previous owner of a cell phone number. Not all communications were therefore necessarily applicable to the research.

Another limitation to consider in the research project is that there was no control over the information processed in line with the RICA Act of 2002 [43] by the store and the service provider from whom the sim cards were purchased. Personal information could also have been leaked during this process.

VIII. CONCLUSION

The objective of this research was to establish if any personal information value chains were created in the insurance industry through the flow of personal information and secondly, whether certain conditions of PoPI were complied with from a marketing perspective. An experimental design was used within the insurance industry of South Africa as a sample population. This was investigated by establishing whether the customer (data subject) was contacted by the companies in the selected sample if they had not opted in for any communication.

The results indicated that 67% of the entities did not have the researcher's consent during the research to contact the researcher. In addition, the senders of 57% of SMSs had not given the researcher the option to opt-out. The researcher was contacted by companies who were not included in the sample, indicating that data could have been shared or leaked. It was also found that the researcher was contacted randomly for ad hoc marketing that was not tailored to the researcher's demographic traits. No significant personal data value chains could be identified.

Future research using a longer time frame is necessary to monitor the data flow, and to further investigate the establishment of data value chains and compliance with PoPI. Additional value will be added if the experiment is repeated once PoPI commences.

IX. REFERENCES

[1] Chen, L.F. and Ismail, R., "Information Technology program students' awareness and perceptions towards personal data protection and privacy", 3rd International Conference on Research and Innovation in Information Systems, ICRIIS, pp. 434–438, 2013.

[2] Doyle, C. and Bagaric, M., "The right to privacy: appealing, but flawed", *The International Journal of Human Rights*, Vol. 9 No. 1, pp. 3–36, 2005

[3] Hiranandani, V., "Privacy and security in the digital age: contemporary challenges and future directions", *The International Journal of Human Rights*, Vol. 15 No. 7, pp. 1091–1106, 2011.

[4] Van der Sloot, B., "Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system", Computer Law & Security Review, Elsevier Ltd, Vol. 31 No. 1, pp. 26–45, 2015.

[5] Goodman, E., "Design and ethics in the era of big data", Interactions, Vol. 21 No. 3, pp. 22–24, 2014.

[6] Borena, B., Belanger, F. and Ejigu, D., "Information Privacy Protection Practices in Africa : A Review Through the Lens of Critical Social Theory", 2015 48th Hawaii International Conference on System Sciences Information, pp. 3490–3497, 2015.

[7] De Bruyn, M., "the Protection of Personal Information Act and Its Impact on Freedom of Information", International Business & Economics Research Journal, Vol. 13 No. 6, pp. 1315–1340, 2014CIBECS, "2012 State of business data protection in South Africa", Available from: http://offers.cibecs.com/state-of-business-data-protection-in-sa, (Accessed 23 March 2015), pp.14, 2012

[8] Milo, D. and Ampofo-anti, O., "A not so private world", Without Prejudice, Vol. 14 No. 09, pp. 30–32, 2013.

[9] Prinsloo, P., Archer, E., Barnes, G., Chetty, Y., & van Zyl, D., Big(ger) data as better data in open distance learning . International Review of Research in Open and Distance Learning, Vol. 16 No. 1, pp. 284–306, 2015.

[10] PricewaterhouseCoopers (PwC), "The protection of personal information bill: The journey to implementation", Available from: https://www.pwc.co.za/en/assets/pdf/popi-white-paper-2011.pdf (Accessed 24 February 2016), 2011.

[11] Greenleaf, G., "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", *Journal of Law, Information & Science*, Vol. 23 No. 1, pp 1-48, 2014.

[12] Olinger, H.N., Britz, J.J. and Olivier, M.S., "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa", International Information and Library Review, Vol. 39 No. 1, pp. 31–43, 2007.

[13] Directive 95/46/EC of the European Parliament and of the Council of 1995. Available from : http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (Accessed 24 February 2016)

[14] General Data Protection Regulation (GDPR) of 2012. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX: 52012PC0011&from=EN (Accessed 24 February 2016).

[15] Hunton and Williams , "The proposed EU General Data Protection Regulation: A guide for in-house lawyers", Available from: https://www.huntonregulationtracker.com/files/Uploads/ Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf (Accessed 24 February 2016), 2015.

[16] Diaz-Tellez, Y., Bodanese, E.L., Nair, S.K. and Dimitrakos, T., "An architecture for the enforcement of privacy and security requirements in internet-centric services", Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012, pp. 1024–1031, 2012.

[17] Protection of Personal Information Act (PoPI) 4 of 2013, South African Government, Available from: http://www.acts.co.za/ consumer-protection-act-2008/index.html (Accessed 20 June 2015).

[18] Promotion of Access to Information Act (PAIA) 2 of 2000, South African Government, Available from: http://www.acts.co.za/ promotion-of-access-to-information-act-2000/index.html (Access 20 June 2015).

[19] Heyink, M., Funds Approved for Establishment of Privacy Regulator, Privacy Online, Available from:http://www.privacyonline.co.za/news/2015/06/Funds_Approved_Establishment_Privacy_Regulator (Accessed 20 June 2015)

[20] Pillay, L., "The partial commencement of the Protection of Personal Information Act , 2013", Without Prejudice, Vol. 14 No. 8, p. 54, 2014.

[21] Wilson, S., "Big data held to privacy laws, too", Correspondence, Macmillan Publishers Limited., Vol. 519, p. 414, 2015.

[22] Magolego, B.N., "Personal data on the Internet – can POPI protect you?", De Rebus, No. 548, pp. 20–22, 2014.

[23] Consumers Protection Act (CPA), 68 of 2008. South African Government, Available from: http://www.acts.co.za/consumer-protection-act-2008/ (Accessed 16 October 2015).

[24] Calaguas, M., "South African Parliament Enacts Comprehensive Data Protection Law: An Overview of the Protection of Personal Information Bill", Africa Law Today, No. 3, pp. 1–6, 2013.

[25] Swart, I.P., Grobler, M.M. and Irwin, B., "Visualization of a data leak", 21st Conference on the Domestic Use of Energy, pp. 1–8, 2013.

[26] Botha, J.G., Eloff, M.M. and Swart, I.. The effects of the PoPI Act on small and medium enterprises in South Africa. In Information Security for South Africa (ISSA), 2015 (pp. 1-8). IEEE, 2015.

[27] Miller, H.G. and Mork, P., 2013. From data to decisions: a value chain for big data. IT Professional, 15(1), pp.57-59.

[28] European Commission. (2013) A European strategy on the data value chain. Retrieved from https://ec.europa.eu/digital-agenda/en/news/elements-data-value-chain-strategy. (Accessed 07 July 2013)

[29] Hamann, B. and Papadopoulos, S., "Direct marketing and spam via electronic communications : An analysis of the regulatory framework in South Africa", De Jure, Vol. 47 No. 1, pp. 42–62, 2013.

[30] Dolnicar, S. and Jordaan, Y., "A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing", Journal of Advertising, Vol. 36 No. 2, pp. 123–149, 2007.

[31] Lai, Y.-L. and Hui, K. L., "Internet Opt-In and Opt-Out: Investigating the Roles of Frames, Defaults and Privacy Concerns", 2006 ACM SIGMIS CPR Conference on Computer Personnel Research, pp. 253–263, 2006.

[32] Bellman, S., Johnson, E.J. and Lohse, G.L., "On site: to opt-in or opt-out?: it depends on the question", Communications of the ACM, Vol. 44 No. 2, pp. 25–27, 2001.

[33] Millard, D., "Hello, POPI? On cold calling, financial intermediaries and advisors and the Protection of Personal Information Bill", Journal of Contemporary Roman-Dutch Law, Vol. 76, pp. 604-622, 2013.

[34] Financial Advisory and Intermediary Services (FIAS) Act, 2002 (Act No. 37 of 2002). Available from: http://www.acts.co.za/ financial-advisory-and-intermediary-services-act-2002/ (Access 5 March 2016).

[35] Widup, S., Bassett, G., Hylender, D., Rudis, B., Spitler, M., "2015 Protected Health Information Data Breach Report", Available from: http://www.verizonenterprise.com/resources/reports/rp_2015 -protected-health-information-data-breach-report_en_xg.pdf, (Accessed 5 March 2016), 2015.

[36] PricewaterhouseCoopers (PwC), "Turnaround and transformation in cybersecurity", Available from: https://www.pwc.com/gx/en/ consulting-services/information-security-survey/assets/pwc-gsiss-2016-financial-services.pdf Accessed 5 March 2016), 2015.

[37] CIBECS, "2012 State of business data protection in South Africa", Available from: http://offers.cibecs.com/state-of-business-data-protection-in-sa, (Accessed 23 March 2015), pp.14, 2012

[38] Brewer, J.D., "The A-Z of Social Research Positivism", SAGE Research Methods, pp. 236–238, 2015.

[39] Cohen, D. and Crabtree, B., The Positivist Paradigm, Available from: http://www.qualres.org/HomePosi-3515.html, (Accessed 27 June 2015), 2008.

[40] Staller, K., "Encyclopedia of Research Design", *Encyclopedia of Research Design: Qualitative Research*, pp 1159-1164, 2010

[41] Miller, R.L. and Brewer, J.D., "The A-Z of Social Research Research design", SAGE Research Methods, pp. 263–269, 2003.

[42] Seltman, H.J., "Experimental Design and Analysis", p. 35., 2013

[43] Regulation of Interception of Communication and Provision of Communication –Related Information Act (RICA), Act 70 of 2002, South African Government, Available from: http://www.acts.co.za/regulation-of-interception-of-communications-and-provision-of-communication-related-information-act-2002/ (Accessed 24 February 2016).