Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Personal information value chains in the South African insurance industry – an experiment

Neriyan Nadasen
University of South Africa, neriyan@gmail.com

Colin Pilkington
University of South Africa, pilkicl@unisa.ac.za

Adelé da Veiga
University of South Africa, dveiga@unisa.ac.za

52. Personal information value chains in the South African insurance industry – an experiment

Neriyan Nadasen
University of South Africa
neriyan@gmail.com

Colin Pilkington
University of South Africa
pilkicl@unisa.ac.za

Adelé da Veiga
University of South Africa
dveiga@unisa.ac.za

Abstract

Personal information is being generated and distributed at an increasingly rapid pace. This phenomenon provides both opportunity and risk in equal measure. The flow of personal information allows corporations to use information about what services are needed and where they are needed. Harnessing the power of this big data can potentially transform society for both corporations and their customers. However, personal information could be exploited for private commercial gain without permission being sought or the individual being informed. It is for this reason that relevant legislation has been passed in South Africa in the form of the Protection of Personal Information (PoPI) Act, bringing South Africa on par with international privacy legislation. This research explores both positive and negative aspects of forming personal information value chains in South Africa by means of an experiment within the scope of the South African insurance industry. This experiment demonstrates the lack of value-adding personal information chains within the industry and it also highlights how information is spread and the importance for the legislation to be strictly enforced to counteract the unauthorised leaking of individuals' personal information.

Keywords

Big data, Protection of Personal Information (PoPI) Act, privacy, personal information value chains, insurance, experiment

1. Introduction

The possession of information is known to provide for a competitive edge (Maitland, Bauer, & Westerveld, 2002) and it is recognised that customers' personal information can be seen as an asset (European Commission, 2013; OECD, 2013). However, alongside this is the acceptance of the right to privacy (Bawa, 2006). There is thus a tension between realising the value offered by the possession of personal information (e.g. name, surname, address, health or financial information) and the privacy concerns of the people whose personally identifiable information it is (PWC, 2016b). Not only must the right balance here be sought (European Commission, 2013), but there is also the realisation that privacy frameworks will have an impact on the value available in personal information (OECD, 2013). The idea of stringing together data from various sources to create a value chain to satisfy an entity's commercial interests is not a new one. Many private companies and corporations have been doing this for a number of years (Evans, 2009). For example, Google has been quite open about their policies of monitoring users' e-mails and web searches in order to target them with specific advertisements (Evans, 2009).

However, in developing countries, governments and companies are still in the embryonic stages of harnessing the power of big data to form personal information value chains in order to better service their citizens and customers respectively. It is this reality that makes this research project both warranted and necessary. There has been no major research into whether personal information value chains exist to provide value for South African citizens and there has been minimal research into whether these personal information value chains are being used to develop and transform both the economy and society at large. A research undertaking that focuses on closing such gaps in knowledge is necessary, but it is also too vast and complex for a single research project. Therefore, this research narrows its focus to concentrate on the South African insurance sector. Key aspects of this research investigate whether there are flows of personal information that can be used to form value chains by private companies, which could then be used in other sectors, including government. Attention is also paid to the privacy of individuals with respect to their personal information in this process of creating value chains.

This paper considers the current state of existing research in big data and personal information value chains in section 2. Following that, two research questions are formulated in section 3. The research methodology used to answer these is explained in section 4. The results are presented in section 5 and the findings discussed and evaluated in section 6. The limitations of the research process and the direction of future work are discussed before concluding in section 7.

2. Background

Data, including personal information, is being collected, stored and analysed at an increasing rate (NESSI, 2012; Villars, Olofson, & Eastwood, 2011). The advent of the internet, as well as social media, e-mail and other communication tools, all of which are now powered by mobile devices, have helped to ensure that the creation of data has increased exponentially (OECD, 2013). This data is commonly referred to as big data (Sagiroglu & Sinanc, 2013) and its volume brings with it benefits and opportunities, on one hand, as well as potential dangers and risks, on the other. Big data can be seen as a business opportunity (Apenteng, 2014; NESSI, 2012) and knowledge (not just data) about current and potential customers is a resource for any company (Crié & Micheaux, 2006). Such views of personal information can even be seen in decisions by regulatory authorities when they expect mobile service providers to carry the cost of required monitoring of communications, which can then be offset against the benefits of the personal information resource that they have access to (Bawa, 2006). However, its use may be seen as opportunistic commodification of such personal information (Donovan & Martin, 2014).

Related to this is the availability of data that the internet has allowed and the ways in which it has changed how business is carried out (Grewal, Iyer, Krishnan, & Sharma, 2003). In the insurance industry, specifically, customers can easily compare prices from different providers (Grewal et al., 2003; PWC, 2016a). As attempts can thus be made via digital channels to beat competitor pricing through lower prices, leading to lower margins, and it could help focus providers on delivering better value (Grewal et al., 2003; PWC, 2016a). Thus, a large percentage of insurance company CEOs consider the speed of technological change as a threat to company growth (PWC, 2016a).

2.1 The use of big data to form personal information value chains

The main factors of big data relate to its volume (the amount of it), velocity (the speed at which it is growing and at which decisions need to be made), variety (numeric, free text, audio, video), variability (inconsistent data flows), complexity (its links to other data) and its value (when exploited) (European Commission, 2013; NESSI, 2012; SAS, 2012). The value comes from harvesting, harnessing (rather than just having) and exploiting this access to big data (Miller & Mork, 2013; SAS, 2012). Advances in technology have allowed the creation of what are termed value chains, where such computer technology is no longer merely a support service, but an integral part of the collection, storage and processing of data, adding layers of value to the raw data and leading to competitive advantage (European Commission, 2013; Porter & Millar, 1985).

The collection of big data, when it is properly mined and analysed, gives companies the ability to make informed decisions regarding their customers, leading to business value (Apenteng, 2014; SAS, 2012). Information becomes inform-action (Crié & Micheaux, 2006). This is because big data enables companies to form patterns and provides them with a "bird's eye" view of data that would otherwise be singular and unrelated (Vaidhyanathan & Bulock, 2014). Indeed, with the creation of a larger and wider data ecosystem of combined and linked data, it should be possible to build up detailed profiles of customers, leading to a better understanding of these customers (European Commission, 2013; OECD, 2013). E-services, which can be defined as combining technology (the internet and mobile devices) and big data to offer services, can be considered an example of such value chains (Prinsloo, Archer, Barnes, Chetty, & Van Zyl, 2015). Similarly, informal traders can use big data and e-services to boost their business and stimulate the local economy as it allows them to not only communicate with each other, but also to receive information from suppliers about deals and discounts (Asongu, 2013). Not only do value chains have the potential to provide benefits in education and health, among others (Apenteng, 2014), but they can also be of benefit to individuals – individuals who are willing to share their personal data could even profit for a portion of the proceeds of the sale of such data (OECD, 2013). The collection and analysis of raw data, with a view to using it within a framework of offering targeted, efficient and useful e-services, form part of a personal information value chain (Crié & Micheaux, 2006; Donovan & Martin, 2014; Miller & Mork, 2013). Personal information value chains should treat each individual as unique (Crié & Micheaux, 2006) and allow companies to direct specific services to customers identified as needing that service, enabling companies to make better strategic and operational decisions in a more efficient manner (Prinsloo et al., 2015), allowing them to attract and retain customers (Grewal et al., 2003). There should thus be a concomitant shift from a product focus to a customer focus, using the personal information value chain to provide strategic marketing and improved value and even encourage loyalty (Grewal et al., 2003; Maitland et al., 2002).

However, considering the potential of big data and personal information value chains, there are both challenges and risks that need to be addressed. Some of the challenges relate to ensuring that the right data is collected as well as establishing its quality (as big data does not imply good data) (Apenteng, 2014; Crié & Micheaux, 2006; Vaidhyanathan & Bulock, 2014). Data fragmentation can also prevent the full realisation of data's value (Miller & Mork, 2013). Furthermore, governments could use this information to aim election campaigns at communities that are most in need (Aker & Mbiti, 2010), thereby using the provision of services as a bargaining chip in exchange for votes. A major challenge facing the wider implementation of e-services is the lack of penetration of the internet in rural parts of Africa. Although the use of mobile phones may have increased internet access, the cost of data may limit the use of the internet for taking advantage of e-services.

2.2 The impact of legislation governing the flow of personal information

Privacy defines the boundaries of an individual's personal space and information and how access across these boundaries is controlled. The advent of big data has led to widespread concern with regard to the threats faced by the privacy of personal information and its irresponsible use for purposes other than for which it was originally collected (European Commission, 2013; Olinger, Britz, & Olivier, 2007; PWC, 2016b). Considering that the capacity to transmit big data doubles every year (Neville, 2000), these concerns are not misplaced. These concerns are given further credence by an incident involving the South African Post Office (SAPO), which, in June 2004, attempted to sell the personal information of customers (Olinger et al., 2007). At the time, its customers could take no legal recourse to prevent this sale.

Appropriate measures are required to ensure the protection of the individual's personal information. The general response internationally has been to draft policies and pass legislation to achieve this (Olinger et al., 2007) and should empower an individual to decide how to use their personal information to gain both private or economic advantage (European Commission, 2013). The South African Protection of Personal Information (PoPI) Act was signed into law on 19 November 2013 and published in the *Government Gazette* on 26 November 2013 (Coetzee, 2015). Customers will benefit from PoPI as they will have more control over who processes their personal information and for what purposes it is used. It further guarantees the right to know when personal information has been processed, who the responsible parties are as well as if the data has been accessed by unauthorised parties (Luck, 2014). PoPI (2013) defines a responsible party as, "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". In the context of this research the insurance companies included in the experiment are regarded as the "responsible parties".

Individuals can also choose that their personal information not be used in marketing campaigns (Coetzee, 2015, PoPI section 69). This may have a significant impact on the insurance industry, as it relies on many direct marketing approaches such as "cold-calling" and e-mail communication to get in contact with potential customers (Wang, Lee, & Wang, 1998). Once PoPI is enforced, this practice will no longer be allowed, as individuals will either have to give their permission for their data to be accessible or be an existing customer of the insurance company in question (Popescou, 2013, PoPI section 69). Furthermore, an existing customer must be able to object, free of charge, to the use of their personal information for marketing purposes and the customer must be able to "opt out" (Popescou, 2013, PoPI section 69(3)). Therefore insurance companies will be severely limited in terms of who they can target when marketing their products and services. A further benefit is that corporations can only retain an individual's personal information for a specific purpose, according to section 3 of PoPI, and once that purpose has been achieved, the corporation needs to destroy the relevant records (Coetzee, 2015, PoPI section 14). Businesses that adhere to PoPI will be able to build relationships based on trust with their customers. This is because the customers can rest assured that their private data is safe with the company in question, as the onus is on the company that stores this data to ensure that it is adequately secured from external threats (Lamprecht, 2015; "POPI: Threat or Opportunity?", 2010).

The implementation challenges that PoPI presents cannot be underestimated. Firstly, one needs to consider what data constitutes personal information. Personal information has been described broadly as "any information relating to an identified or identifiable individual" (OECD, 2013, p. 7, PoPI 2013). However, would an IP address be considered personal information (Luck, 2014)? It might well be if the definition of PoPI is considered, since an online identifier is included in the definition of personal information. Another issue is that the speed at which technology is created to harness these massive data stores is far outstripping the speed at which legislation is passed to protect against the misuse of the data in question (Hiranandani, 2011). It also needs to be noted that, in some quarters, there is the opinion that certain regulations are a step backwards, as they constrain the flexibility of business to use such personal information in a value chain to remain competitive (NESSI, 2012).

3. Research questions

Big data brings with it both potential benefits and risks. Although insurance companies have always possessed the personal information of their customers, there has been an increased focus on leveraging this information to increase efficiency and effectiveness in terms of services delivered. This personal information can be used to form value chains that can lead to a competitive advantage. However, maintaining the confidentiality of this information has proved a challenge. Until recently, an individual's personal information could be shared without consent and it is yet to be shown how PoPI would affect the flow of personal information through the South African economy in general and the insurance industry in particular.

There are thus two research questions relating to the South African insurance industry that will be addressed in this paper.
(1) Can any personal information value chains be found in the flow of personal information?
(2) Is the privacy of personal information of customers respected?

This paper is part of a larger study of privacy and value chains conducted as a BSc or BCom Honours (the fourth year of study) research project in the School of Computing at Unisa. It is restricted to the insurance industry (whereas other parts of the study considered other sectors in the economy) and only a subset of such insurance companies was included in the study. As PoPI has only recently been promulgated and no commencement date has been given, many insurance companies are still in the process of becoming PoPI compliant. Thus, it is possible that the behaviour of an insurance company with respect to their customers' personal information may have changed during the course of the research timeframe.

4. Methodology

The research was carried out using an experimental design and the necessary ethical clearance to pursue this research was obtained. Experimental research is the best means to determine if a particular action or treatment has any effect on the outcome of a process. This is done by forming two groups: an experimental group, to which the treatment or action is applied, and a control group, to which the action is withheld (Creswell, 2013). This research design would allow for the placing of data with insurance companies and for a "customer" to opt-in or opt-out for further marketing communications (forming the experimental and control groups respectively) and then to consider if there are any differences in the communications that are received via the provided contact channels.

Personal information was deposited onto the websites of a convenience sample of twenty prominent South African insurance companies using six contacts (see Figure 1). Contacts 1 and 2 were both linked to separate cellular phone numbers and e-mail addresses and were both deposited at 10 company websites. Contact 1, a male persona, gave the companies permission to contact the phone number/e-mail address through the opt-in feature, whereas contact 2, a female persona, denied this permission via the opt-out feature, thus forming a control group. Contacts 3 to 6 used only e-mail addresses, where contacts 3 (male) and 4 (female) opted-in and contacts 5 (male) and 6 (female) opted-out, and these were deposited at a further 10 insurance company websites. The two cellular phone numbers used were newly registered for the purposes of this experiment and the 6 e-mail addresses were also newly created specifically for the research.

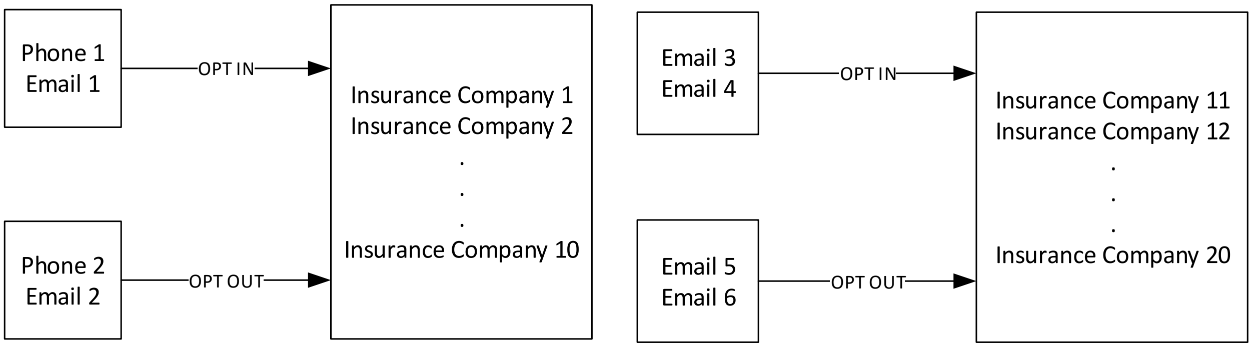

Figure 1: The data depositing strategy

The contacts were deposited onto the insurance websites by way of requesting online quotes and "Call me backs". This ensured that the insurers in question had access to the phone numbers and e-mails addresses of the prospective customers. The data was deposited onto all websites within a 24-hour window. This was done in order to give all phone numbers/e-mail addresses an equal time in the hands of insurers. Once the data was deposited, all communications received via the phone number or e-mail address in question were recorded. For the purposes of the experiment, only communications that occurred between 1 June 2015 and 20 December 2015 were considered. This time frame was determined by the requirements of the research project course of which the experiment was a part. The data collected for each contact was analysed to determine the following:

- What kind of information was received via a contact?

- Did the information received concern products offered by the company in question?
- Did the companies with whom data was deposited respect the privacy of the data?
- Did the companies respect the opt-in/out-out choices made by a contact?

5. Results of depositing data on company websites

Communications received via the cellular phones and e-mail addresses were recorded and categorised. Communications that were from the insurance company where the data had been deposited were considered valid; communications that were from companies that were not part of the sample were considered leaked. See Figure 2 for the consolidated results. Note that no communications were received for contact 6 – it is unlikely that the choice to opt-out of receiving further communications was adhered to (as communications were received via contact 5, which was deposited in the same places as contact 6), but rather that there must have been some technical error with this e-mail address.

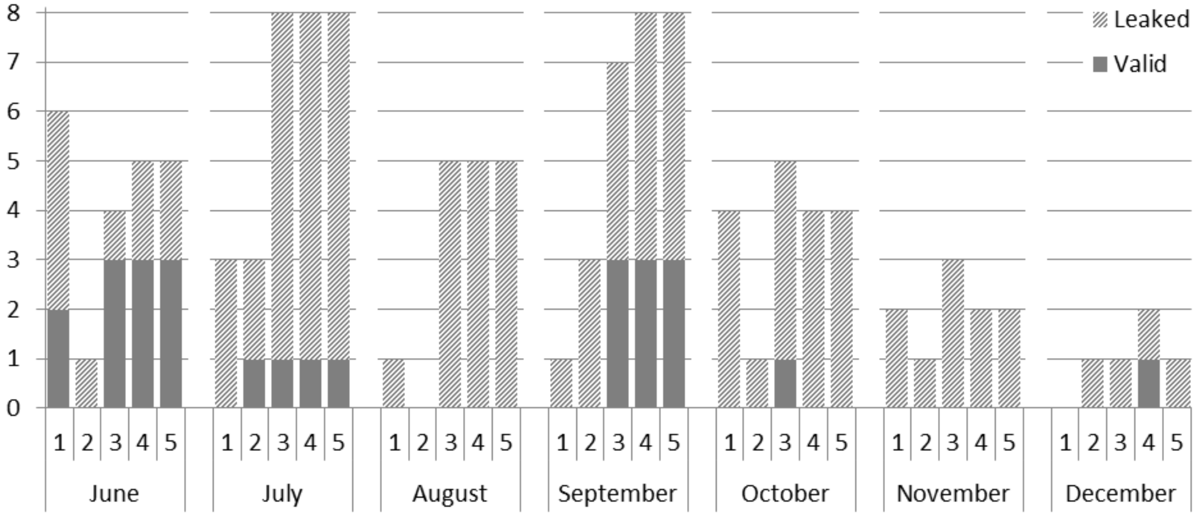

Figure 2: Number of valid and leaked communications received, per contact, per month

It can be seen that communication was more sustained in the first four months after the contact information had been deposited on the company websites and that, thereafter, the volume of communications started dropping. It does need to be noted that for contacts 1 and 2 (where both cellular phone and e-mail details were provided), the service providers preferred communicating via SMS, with only two of the communications for contact 1 being sent via e-mail (in June). It is further noteworthy that it is these two e-mails that accounted for the only valid communications for contact 1 in June (that is, communication from the insurer where the data was deposited and where the opt-in for future communication option was accepted); this could also then explain why contact 2 did not receive similar e-mails, as communication had been opted-out. It is also clear that, on the whole, where only e-mail was used as a communication method (for contacts 3, 4 and 5), more e-mail communication was received, rather than the SMS communication route. The similar pattern of communications for these three contacts is expected, considering that they were all deposited at the same websites (even though the opted-out option for contact 5 had been selected).

For the two contacts (1 and 2), where both cellular phone and e-mail addresses were provided, virtually all communications via SMS were leaked, offering services and products from vendors with which data had not been shared. These leaked SMSs came from other insurance providers as well as other industry sectors – see Table 1 for a breakdown of the number of communications. It is clear that, although contact 1 had opted-in to receive further communications from the insurers in question, the phone number had been passed on to entities outside of this agreement and data privacy had therefore not been respected. The only valid SMS was received by contact 2 in July (even though this contact had opted-out). However, contact 2's phone details had also been passed on to external entities (with only one overlap with those that had communicated with contact 1) and privacy not respected.

	Insurance	Finance	Retail	Mobile content	Gambling
Contact 1	9	2	3	1	0
Contact 2	2	6	0	0	1

Table 1: Number of leaked communications received via SMS by contacts 1 and 2

Contacts 3, 4 and 5 used only an e-mail address and therefore all communication activity is made up purely of e-mail activity. Contacts 3 and 4 opted-in for communication, with contact 5 opting-out, and there is little consistent pattern to the valid communications received during the time of the experiment. Further, although these were all deposited on the same company websites, the e-mails received were not received by the three e-mail addresses in all cases, although there was some overlap, with a greater overlap present between contacts 4 and 5; however, the e-mails were mostly from the same 3 insurers in all cases (with only 1 other insurer e-mailing contact 3). These valid e-mails advertised products and services that are offered by the insurers as well as special limited offers. Although these communications were solicited (for the opted-in contacts 3 and 4), the automated and non-personalised nature of the e-mails, combined with the generic content, imply that they could have been part of a direct marketing campaign. Therefore, one can argue that the information provided to the insurers was not used to offer a customised product or service. Considering that contact 5 had opted-out, there should have been no valid further communication via this e-mail address, which was not the case, and one can conclude that the opt-out instruction was not adhered to.

	Insurance	Finance	Airline	Automotive
Contact 3	20	4	1	0
Contacts 4 & 5	19	5	1	1

Table 2: Number of leaked communications received via e-mail by contacts 3, 4, and 5

The e-mail communication resulting from data leaks appear to be much more focused on the insurance sector (see Table 2) and was identical for contacts 4 and 5, with an 80% overlap with contact 3. These e-mails far outnumber those that were solicited and the privacy of the data was not maintained for these three contacts. Again, the companies to which the data was leaked were sending generic mass marketing e-mails, with no clear pattern in the dates on which the e-mails were sent. Therefore, the choice of either opting-in or opting-out did not seem to make a difference in upholding the customer's preferences concerning privacy.

6. Discussion of the results

The results are discussed by answering the two research questions and examining them in terms of results presented above. As contact 6 had no communications, it is not commented on further.

6.1 Personal information value chains

The definition of a personal information value chain implies that raw data has been processed by a private or government organisation by applying business rules to the raw data, resulting in valuable information, which gives the company or government organisation an advantage in fulfilling its mission. Based on the results of the experiment, it is evident that personal information value chains are almost non-existent in the South African insurance industry. In the cases of contacts 3, 4 and 5 the contact details were leaked to other insurance companies, so it could be argued that the beginnings of a personal information value chain were being formed.

Also, the advantages of digital platforms and new technologies mean that businesses can move past the one-to-many approach of traditional marketing approaches to target customers in a more individualised or segmented manner (OECD, 2013). However, the random nature of the communications received from these external entities seemed focused on generic mass marketing rather than extracting information with the aim of forming a value chain to provide the customer with a specialised offering fitting the customer's profile. Although differing personal information was deposited on the company websites, insurance companies and other external entities did not use these differences to refine their list of recipients in order to target individuals with a suitable product. Even in the cases where there was consent to receiving further communications, insurance companies sent generic e-mails that did not offer a customised product based on the personal data submitted. So, while personal information value chains can lead to new business models (Apenteng, 2014), it does not appear to be the case here. Using the personal information provided, the insurance companies could have formed a profile of the user and sent out communications offering products and services that best suit the needs of the customer. During the data depositing process, insurance companies were provided with raw data such as name, surname, address, age and profession, among others. The insurance companies in question could have extracted value from this data to form a personal information value chain. This value chain could then have been used to target personalised communications instead of the generic special offers and deals that were sent out.

6.2 Respecting privacy

It is clear from the results of this experiment that the right to privacy was not maintained. Of the total number of communications received, 80% were from unsolicited, leaked service providers, and were thus the product of personal information that had been passed on without the permission of the owner of that data. This goes up to 86% when the unsolicited communications from valid, opted-out, sources are included. Further, it appears irrelevant whether one opts-in or opts-out, as the various contact details were leaked to external entities for all contacts, which then proceeded to use these contact details in marketing campaigns.

It should be noted that such unsolicited direct marketing is explicitly prohibited by PoPI, section 69 (2013) and that non-compliance with the terms of the act could lead to fines and even imprisonment (section 107, "Protection of Personal Information Act", 2013). It is of concern that only 50% of insurance company CEOs note that customer personal information security is a priority in terms of their relationship with their customers (PWC, 2016a), even though such privacy is a common concern for their customers (Crié & Micheaux, 2006). Furthermore, where privacy legislations does exist, its implementation and enforcement may remain limited in some, particularly developing, markets (Donovan & Martin, 2014).

6.3 Limitations and future work

Some limitations need to be highlighted and could be used to develop this research further. Firstly, a longer timeframe is necessary to obtain a more accurate reflection of whether there are personal information value chains in operations in the South African insurance sector and since trends or patterns could take many months to form with respect to the manner in which communications are targeted. It is expected that this would increase the activity across all contacts. Secondly, the use of social media, combined with mobile devices, is driving the production and consumption of big data and its inclusion could have led to a wider assessment of the creation of personal information value chains. Thirdly, the recycling of mobile numbers (the allocation of an inactive mobile number to a new subscriber) could also have affected the experimental data as a previous subscriber may have opted-in to receive communications from a specific company, which may not be aware that the mobile number is no longer used by the individual that opted-in. Additionally, it is also important to note that the form the experiment took could not determine how many or which companies leaked personal data and to whom. Also, the mobile service provider may have compromised the privacy of the contact details. This makes it almost impossible to determine if the personal information was leaked by the insurance companies or the mobile provider. Finally, progressive implementation of PoPI could mean that a company's behaviour with respect to personal information may have changed over the course of the experiment.

7. Conclusion

Personal information value chains refer to the process of handling such data holistically from the point of capture to final strategic decisions (Miller & Mork, 2013). The aim of this research was to identify whether opportunities for personal information value chains that arise in the insurance industry are being realised. This was achieved by determining whether raw data has been transformed into knowledge that adds value to a company with the view to offering enhanced services to customers in the insurance industry. Also, could sharing information with various insurers be done while maintaining the individual's privacy?

It is hard to ignore the strategic importance that technology offers business through the process of creating personal information value chains (Porter & Millar, 1985). Yet this research indicates that the South African insurance industry is yet to develop processes that create such value chains from the raw data that is at their disposal. The experiment that was carried out demonstrated the current methodology that is used to communicate with potential customers seems to be largely based on mass marketing without any regard for the individual's specific needs. Both insurance companies and customers have plenty to gain if data can be leveraged in an efficient manner. Further, benefitting from the affordances of having access to the personal information of potential customers need not be achieved while ignoring the privacy of such data (NESSI, 2012); however, the mass marketing was carried out without maintaining the privacy of the data gathered, even when it was explicitly asked for (via the opt-out feature).

This research project helps to bring both the niche area of the South African insurance sector, as well as the uptake of big-data-leveraging methods as a whole, to the fore. The paper highlights where South African insurance companies could be falling short in the areas of privacy and personal information value chains, with the intention of guiding further development and research in this area. The lack of privacy afforded to an individual's personal data is shown to be a hurdle that needs to be overcome and further research into this occurrence should be conducted once PoPI is fully implemented.

References

Aker, J.C. and Mbiti, I.M. (2010) "Mobile phones and economic development in Africa", *Journal of Economic Perspectives*, 24(3), pp. 207–232.

Apenteng, S.A. (2014) "Big Data : A tool for development in developing nations", *International Journal of Scientific and Research Publications*, 4(5), pp. 1–5. Retrieved from http://www.ijsrp.org/research-paper-0514/ijsrp-p2967.pdf

Asongu, S.A. (2013) "How has mobile phone penetration stimulated financial development in Africa?", *Journal of African Business*, 14(1), pp. 7–18.

Bawa, N. (2006) "The regulation of the Interception of Communications and Provision of Communication Related Information Act" in L. Thornton, Y. Carrim, P. Mtshaulana, & P. Reyburn (eds.), *Telecommunications Law in South Africa*, Johannesburg: STE, pp. 296–333.

Coetzee, M. (2015) "Why should my business be PoPI compliant?", *EngineerIT*.

Creswell, J.W. (2013) *Research design: qualitative, quantitative, and mixed methods approaches*. Thousand Oaks: SAGE Publications.

Crié, D., and Micheaux, A. (2006) "From customer data to value: What is lacking in the information chain?", *Journal of Database Marketing & Customer Strategy Management*, 13(4), pp. 282–299. doi:10.1057/palgrave.dbm.3240306

Donovan, K.P. and Martin, A.K. (2014) "The rise of African SIM registration: The emerging dynamics of regulatory change", *First Monday*, 19(2). doi:10.5210/fm.v19i2.4351

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

Evans, D. S. (2009) "The online advertising industry: economics, evolution, and privacy", *Journal of Economic Perspectives*, 23(3), pp. 37–60.

Grewal, D., Iyer, G.R., Krishnan, R., and Sharma, A. (2003) "The internet and the price-value-loyalty chain". *Journal of Business Research*, 56(5), pp. 391–398. doi:10.1016/S0148-2963(01)00227-2

Hiranandani, V. (2011) "Privacy and security in the digital age: contemporary challenges and future directions", *The International Journal of Human Rights*, 15(7), pp. 1091–1106.

Lamprecht, I. (2015) "Four regulatory reforms you should know about". *Personal Finance*, 409, pp. 8–9.

Luck, R. (2014) "POPI - Is South Africa keeping up with international trends?", *De Rebus*, 541, pp. 44–46.

Maitland, C.F., Bauer, J.M., and Westerveld, R. (2002) "The European market for mobile data: Evolving value chains and industry structures", *Telecommunications Policy*, 26(9-10), pp. 485–504. doi:10.1016/S0308-5961(02)00028-9

Miller, H G., and Mork, P. (2013) "From data to decisions: A value chain for big data", *IT Professional*, 15(1), pp. 57–59.

NESSI. (2012) *Big data. A new world of opportunities*. *NESSI White paper*. Retrieved from http://www.nessi-europe.eu/Files/Private/NESSI_WhitePaper_BigData.pdf

Neville, E. (2000) "The public's right to know - the individual's right to privacy", *Policing and Society*, 9(4), pp. 413–428.

OECD. (2013) *Exploring the economics of personal data: a survey of methodologies for measuring monetary value*. *OECD Digital Economy Papers*. doi:10.1787/5k486qtxldmq-en

Olinger, H N., Britz, J J., and Olivier, M.S. (2007) "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*, 39(1), pp. 31–43.

Popescou, T. (2013) "Two's company and three's a crowd", *Without Prejudice*, 13(7), 71–72.

"POPI: Threat or opportunity?" (2010) *Enterprise Risk*, 4(6), pp. 22–24.

Porter, M.E., and Millar, V.E. (1985) "How information gives you competitive advantage". *Harvard Business Review*, 63(4), pp. 149–160.

Prinsloo, P., Archer, E., Barnes, G., Chetty, Y., and Van Zyl, D. (2015) "Big(ger) data as better data in open distance learning", *International Review of Research in Open and Distance Learning*, 16(1), pp. 284–306.

Protection of Personal Information Act. (2013). Government Gazette, Vol. 581, No. 37067, Act No. 4 of 2013. Cape Town, South Africa.

PWC. (2016a) *Seizing the future. 19th annual global CEO survey. Key findings in the insurance sector*. Retrieved from http://www.pwccn.com/webmedia/doc/635908668405519628_annual_global_ceo_survey_19th_insurance.pdf

PWC. (2016b) *Turnaround and transformation in cybersecurity. Key findings from The Global State of Information Security Survey 2016*. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

Sagiroglu, S., and Sinanc, D. (2013) "Big data: a review". *2013 International Conference on Collaboration Technologies and Systems (CTS),* pp. 42–47.

SAS. (2012) *Big data meets big data analytics*.

Vaidhyanathan, S. and Bulock, C. (2014) "Knowledge and dignity in the era of "big data". *The Serials Librarian*, 66(1-4), pp. 49–64.

Villars, R. L., Olofson, C. W., and Eastwood, M. (2011) *Big data: What it is and why you should care*. IDC White paper.

Wang, H., Lee, M.K.O., and Wang, C. (1998) "Consumer privacy concerns about internet marketing", *Communications of the ACM*, 41(3), pp. 63–70.