Ethical and Legal Issues Involved in the Pro-active Collection of Personal Information with the Aim of Reducing Online Disclosure

Johnny Botha[1,2(✉)], Mariki Eloff[1], and Marthie Grobler[2]

[1] Institute for Corporate Citizenship,
University of South Africa, Pretoria, South Africa
eloffmm@unisa.ac.za
[2] CSIR, Pretoria, South Africa
{jbothal,mgroblerl}@csir.co.za

Abstract. Pro-actively finding leaked information online can potentially reduce detection times to limit the exposure time of personal information on publicly accessible networks. Often the breaches are discovered by an external third party and not the data owner. The time that data is exposed on the Internet has severe negative implications since a significant amount of information disclosed in a data breach has been proven to be used for cybercrime activities. It could be argued that any reduction of data breach exposure time should directly reduce the opportunity for associated cyber-crime. While pro-active breach detection has been proven as potentially viable in previous work, several aspects of such a system still need to be investigated. This paper aims to highlight some of the major ethical and legal issues when pro-actively collecting personal information, through a South African case study, to assist in reducing the amounts of personal information being disclosed online.

Keywords: Data breach · Ethical and legal issues · Privacy · Personal · Identifiable information

1 Introduction/Background

Data breaches occur more frequently nowadays and are becoming an inescapable risk factor for individuals and organisations [1]. In the event of a data breach, large amounts of personal data, often intimate details, may be exposed. Cyber criminals and hackers are regularly making use of these Personal Identifiable Information (PII) obtained by exploiting it in numerous ways such as identity theft, spamming, phishing and cyber-espionage [2]. Detecting and removing exposed data is therefore of utmost importance; yet the average breach remains undetected on average in excess of three months [3].

Privacy laws are being instantiated internationally to serve as a safeguard of PII. For example, in South Africa the Protection of Personal Information (PoPI) Act has

D. Kreps et al. (Eds.): HCC12 2016, IFIP AICT 474, pp. 72–85, 2016.
DOI: 10.1007/978-3-319-44805-3_7

been adopted in November 2013 [4]. South Africa needs to make use of this new legislation to make adjustments to the way information is stored and processed by organisations that are not yet compliant to the Act. The possibility of pro-active automated breach detection is discussed in previous work as a mechanism to potentially reduce detection times to limit the exposure time of PII on publicly accessible networks. The aim of the pro-active collection process is to highlight the amount of PII being disclosed online in order to assist in the reduction of the information being leaked, whether by choice or coercion. However, an operational pro-active detection system may give rise to ethical and legal issues. This paper focusses on some of these issues when pro-actively collecting PII online. Although pro-active detection of data breaches is internationally applicable, this paper will investigate ethical and legal issues in pro-actively collecting PII through a South African case study, based on the relative newness of the South African PoPI Act. While the results of a previous experiment on the pro-active detection system focus on the South African landscape (refer to Sect. 2), the system is capable of assisting in global ethical application and privacy regulation that is customised to country specific requirements.

2 Pro-active Data Breach Detection

In order to gauge the level of existing PII disclosure before the promulgation of the PoPI Act, a custom developed software application, called Cyber Protect, was used in an experiment to pro-actively scan the Internet in search of leaked PII in 2014, shortly after the PoPI Act was put in place. Another experiment was conducted in 2015 to determine how effective the PoPI legislation is in reducing the amounts of PII detected online. This was done by collecting datasets using the custom application and examining the results for indicators of how effective the PoPI legislation has been since its inception. These experiments will be referred to as previous work performed [5]. This paper will investigate the ethical and legal issues based on the results of these experiments.

2.1 Application Architecture

The application serves as a PII detection and collection service that is capable of scanning the Internet for PII that are being disclosed in electronic documents. In this context, a scan on the Internet refers to the application making use of public data sources, provided by Google, Bing and Twitter. Application Program Interface (API) calls are being used in search of PII being leaked within electronic documents found freely available on the Internet. These documents are stored within the website domain space. For the scope of the experiment performed in the previous work, the scans were limited to the co.za domain [5]. Further data processing takes place in order to obtain an IP address and approximate geo-location for each website found responsible for disclosing personal information. Figure 1 shows the architecture of the custom application.

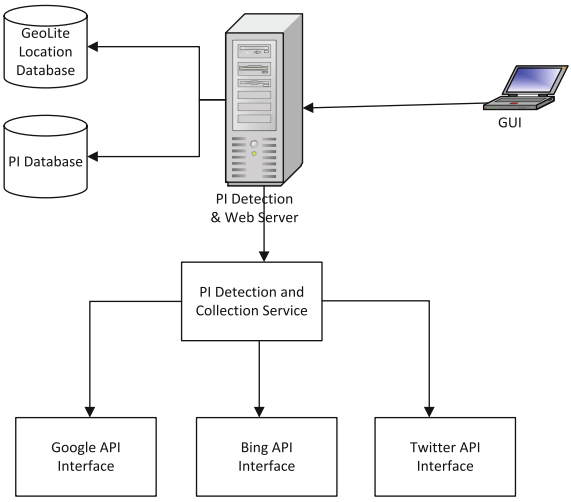

Fig. 1. PII detection application [5]

The type of PII extracted during the experiment was limited to South African Identity (ID) numbers, land line numbers, cell phone numbers, email addresses, credit card numbers and addresses. Other personal information such as names, job location or religious believes requires significant lexical analysis since no dominant standard of identification currently exists. The electronic documents scanned were limited to the most commonly used files such as Text, MS-Word, MS-Excel and PDF files, as well as SQL scripts and XML files. These file types are identified to be most likely responsible for the leakage of PII. Information might reside in other formats, but each document type has unique characteristics that need to be catered for on a technical level and this adds significant overhead to development time that will be addressed in future revisions of the application [5].

2.2 Information Visualisation

The application has a staged approach where information is first collected, then processed and lastly visualised. The image presented in Fig. 2 illustrates how a single server responsible for the leakage of PII is presented by a blue antenna icon with its approximate geo-location. When multiple servers in the same area are found, they are grouped together with the count of servers displayed in the grouped icon as shown in Fig. 2. A count of 234 servers was found in South Africa.

Zooming into the map allows for the opening of specific server nodes and displays more details on that particular server. Figure 3 shows the details on a website URL that

Fig. 2. PII visualisation [5] (Color figure online)

has been opened in the application, indicating that the particular website is responsible for leaking 171 telephone numbers and nine cell phone numbers. The approximate geo-location for this web-server is identified as Durban, South Africa. The complete URL for the file found is hidden due to privacy reasons.

The application only makes use of the limited free queries provided by each of the data sources. This was a deliberate limitation on the research team's part to investigate what could be achieved with little to no resources in terms of pro-active data breach detection. A further study comparing the current free results obtained with a funded approached will be conducted in future work.

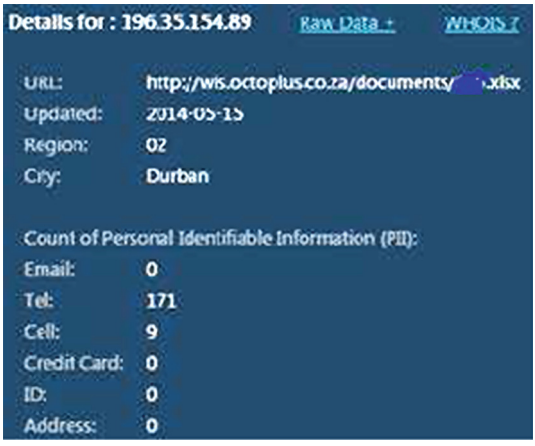

Fig. 3. PII details [5]

3 Personal Information Detected

Two datasets were collected by using the application. Both datasets were collected over a three month period. The first dataset was done six months after the instantiation of the PoPI Act [4]; the second dataset was done one year and eight months after the instantiation of the Act. A general hypothesis would be that the amounts of leaked personal information should have decreased [6].

The automation of data processing and the ease of online transactions have generated increased opportunities to commit various offences (often financial cybercrimes) with personal and financial information [7]. Examples of personal information which is targeted online include:

- Address and phone details, dates of birth and identity numbers can be used to commit identity theft if combined with other information. Having access to information such as a date of birth and address of a person can help the perpetrator to circumvent verification processes.
- Financial information or data is a popular target in cyberspace. Financial information or data which is targeted in cyberspace are information regarding saving accounts, credit cards, debit cards and financial planning information.

The findings from the application on the amounts of leaked PII of both datasets in the experiments indicate that the amounts of PII disclosed in 2015 have slightly increased as the country progress further into the PoPI Act online compliance timeframe [5]. Using the custom detection system, it is possible to geo-locate the webservers or hosts found responsible for the disclosure of PII. A notable finding is that 10718 hosts or servers were detected as responsible for the leakage of personal information. If it is assumed that each

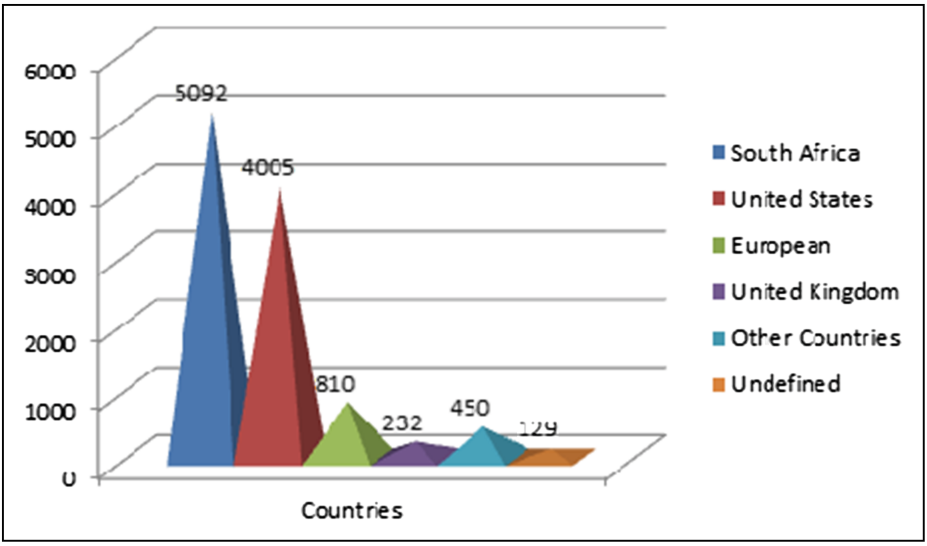

Fig. 4. Host count per country of leaked PII [5]

individual server represents an individual or company, it points to 10718 transgressions of privacy protection legislation. Figure 4 shows a breakdown of the number of hosts found per country. Although the focus is only on South Africa and the co.za domain, the websites can be hosted outside the borders of South Africa. This could highlight non-compliance issues as the PoPI Act (condition 6 Section 18(g)) states that PII may not be stored at international locations without the consent of the data subject [4].

Taking into consideration the time period since the instantiation of the Act and the amount of PII data leaked in 2014 and 2015, one can see that the privacy legislation has very little effect on the amounts of PII data being leaked. It seems that South Africa still has a long road ahead towards the compliance process and possible improvements on the Act to better control the amounts of personal information being leaked.

4 Ethical and Legal Aspects of a Pro-active Detection System

In the digital era, protecting personal information online can be a daunting task. Therefore, having a system in place that could detect the online leakage of PII could be very beneficial. The purpose of the proposed system is to detect leaked or disclosed PII online, regardless of whether the disclosure is a result of inadvertent or malicious actions. To accomplish this, personal data needs to be collected from the Internet with the use of public data sources and analysed.

In order to fully utilise the potential of the system to pro-actively collect personal information online in a legal and ethical manner, an analysis of the relevant ethical and legal aspects should be done. The collection and processing of personal data should be done in such a way that it complies with applicable privacy laws.

4.1 Ethics

Ethical behaviour can be regarded as a set of rules that establishes the boundaries of generally accepted behaviour and is often loosely based on legislative measures [8]. Due to the large dependence on human nature and behaviour, ethics often presents contradictions in terms of two sets of acceptable behaviours, or the application of existing ethical rules in new situations. A company's policy for tracking employee email and Internet usage, for example, stands largely contrasted by the support of personal privacy. Legislation may cover both sides of the argument - the need of the company to protect its resources by ensuring valid use thereof, as well as an individual's right to privacy. The ethical aspects also need to inspect a variety of other related factors. A situation may arise where the law offers little or no guidance and the decision-maker has to do what is regarded as ethical in the situation.

Especially when dealing with customer data, strong measures are required to avoid the development of customer relationship problems. The collection of PII from individuals is often done with the intention of the company to make better decisions in serving the individual, for example, banks require personal information to verify the identity of an individual before performing sensitive financial transactions. However, this should be done in balance with the needs of the individual to have his/her rights and desires protected and adhered to since the use of information technology can lead

to a potential violation of right to privacy. According to the South African Constitution, the right to privacy is put in place to protect an individual. The detection system addresses the protection of an individual's name or likeness through identity theft, by collecting leaked PII online and creating awareness in terms of online data leakage.

4.2 Legal Aspects

Laws and regulations are put in place to prescribe the required conduct in given situations. As such, governments around the globe have been assigned the responsibility of protecting personal and sensitive data of consumers and companies [9].

In terms of privacy on the Internet, five privacy laws are applicable in South Africa:

- The common law dictates that the right to privacy is recognised as an independent personality right that is protected by the South African law of delict. This requires that an infringement must be wrongful (as opposed to be only an act of omission) and determined by the *boni mores* or reasonableness criterion [10].
- The Constitution enforces rights such as the right of respect for privacy. Three obligations are in place, but only the horizontal obligations, where all persons (natural and juristic) have a general duty to respect these rights in their everyday interaction, are applicable to the application.
- The Electronic Communications and Transactions (ECT) Act contains universally accepted data protection principles setting out how personal information may be collected, used and disclosed. These principles are not enforced and thus the adherence to these is voluntary [10].
- The PoPI Act aims to promote the direct protection of personal information processed by both public and private bodies (thus focusing on the obligations as set out by the Constitution). It further introduces certain conditions in which personal information may be processed, and put in place an Information Regulator in South Africa [4]. The PoPI Act prescribes eight conditions or principles under which personal information may be processed (refer to Table 1).

4.3 Ethical Issues Mapped to Legal Issues

Looking at the current implementation of the proposed system, the biggest concern is the fact that the system actively searches for leaked PII on the Internet. Depending on the interpretation of the applicable legislations, it is questionable whether this is allowed. However, the purpose of the system is to identify leaked content and the location of the responsible servers in order to have it removed from the Internet. Although the system is not responsible for the data breach, it does access the data and as such, is in possession of data that may be leaked as a result of either inadvertent actions or criminal activity. Since it is imperative that the system adheres to all South African privacy legislation (refer to Sect. 4.2), it is necessary to analyse the legal requirements and map the potential ethical issues on these. Table 1 shows the applicable South African legal principles related to PII with the respective ethical

Table 1. Legal principles related to PII and ethical implications

Legislation	Legal principle	Ethical implication
Common law	*Boni mores* criterion	In the event of a data breach, should the rights of the breached company or the rights of the individuals take higher preference? For example, the disclosure of breach information related to a listed company would probably have a negative impact on the company's stock. Should the individuals whose PII were breached be notified at all costs, or should the economic stability of the entity rather be protected?
Constitution	Horisontal obligation	The application should not be made available to the general public, due to the collated repository of PII made available through the system interface. However, the application only makes use of freely available data sources in collecting information, and as such it can be argued that it does not impose further infringements than when the PII was found on the Internet
ECT Act	Opportunity to review, correct and withdraw	Any affected data subject who has been identified can ask for information being found on themselves and it will be provided if found in the system. Since people are not being notified at this stage, no one is requesting access to the information being found
	Personal information collection	Since the system makes use of freely available data sources, the data participant does not give express written permission for the data collection by the system. In addition, since the system is not the original source of the leaked information, the system does not notify the person whose information was leaked on the purpose of the system
PoPI Act	Accountability	The system owners are accountable to ensure that the system adheres to the principles of PoPI
	Processing limitation	In the intended operation of the proposed system, by default no consent is given by the data participant. Although the system makes use of freely available data sources, is it ethical to proceed with the collection of the PII, even if the intention is to assist the process of identifying data breaches?
	Purpose specification	The purpose of the proposed system is to highlight the amounts of PII being leaked in order to assess whether the PoPI Act has any effect on the leakage amounts as time progresses. The proposed system enables the identification of

(*Continued*)

Table 1. (*Continued*)

Legislation	Legal principle	Ethical implication
		the person responsible for a specific server (through the WHOIS lookup function), and thus the de-identification condition is not strictly adhered to
	Further processing limitation	Any further processing of the PII should be compatible with the purpose of the collection. The system allows further data processing to obtain an IP address and approximate geo-location for each website found responsible for disclosing PII. The purpose is to assist in the process of eliminating leaked PII, and as such, the system adheres to this
	Information quality	Reasonable steps must be taken to ensure that the PII is complete, accurate and not misleading. Since the proposed system does not make any changes to the retrieved PII, this is not applicable. However, a large number of phone numbers and email address are false positives. For example certain email addresses found were found in documents used as marketing material and therefore does not count as leaked PII
	Openness	Documentation regarding all processing operations must be maintained and the data subject be notified when PII is collected. At this stage the affected parties are not being notified. The purpose is only to keep count of the amounts of PII being leaked since the inception of the Act. The intention is to eventually notify parties involved, but as this paper states there is certain legal and ethical issues involved in doing so
	Security safeguards	Security measures should be in place in terms of integrity and confidentiality of PII, and notification should be given of security compromises. Collected data is stored in a secure environment not accessible by the public or any unauthorised parties
	Data subject participation	Any affected data subject who has been identified can ask for information being found on themselves and it will be provided if found in the system. Since people are not being notified at this stage, no one is requesting access to the information being found

implications, as compiled by the authors. These principles and implications are derived from various sources [4, 9, 10].

Looking at the ethical implications of using such a system on an international level, the PoPI Act is largely representative of the EU Data Protection Directive [11, 12]. Comparing the PoPI Act to the UK Data Protection Act (DPA), USA privacy laws and AUS privacy laws, a lot of similarities were found in the principles of these Acts [11]. This would imply that the same ethical implications will apply if the system was to collect information in Europe, the UK, USA or Australia.

5 Using the Detection System in an Ethical and Legal Manner

Using the system in an ethical and legal manner, it might be possible to reduce the amount of online PII disclosures.

5.1 Addressing Legal and Ethical Aspects

Non-compliance with laws has set results, whilst non-compliance with ethical rules is less predictable [13]. However, as noted in Table 1, the ethical implications raised allows for interpretation based on a set of circumstances. The use of such a detection and collection system by government, industry and an individual user will be theorised. Regardless of the user type, the legal principles listed in Table 1 are non-negotiable and the system has to adhere to this.

Depending on the purpose, a government department using the system may be faced with a variety of ethical issues and legal issues. For the most part government departments are kept accountable for the PII in their possession through the office of the South African Auditor General. This office plays an oversight role to ensure that government adheres to all applicable regulations.

Depending on the purpose, a business using the system may be faced with a variety of ethical and legal issues. Similar to government use, businesses are held publicly accountable for the PII in their possession. Businesses generally have codes of conduct and formal mandates in place, giving the use of such a detection system more credibility. The biggest concern with regard to corporate use would be the intention, and as such, the industry of the business. It would be ethically more acceptable for a law firm or technology company to make use of such a system. A company in the medical or hospitality industry may be frowned upon since the link to their purpose of the developed system may not be clear.

An individual using the system may be faced with a variety of ethical issues. Although the purpose of using the system may be to assist in awareness of leaked PII with the intention of having it removed online, an individual in possession of potentially millions of records of PII may be faced with ethical problems, even if all legal aspects are addressed. Without the regulatory backing of government or the accountability of a business, it may be frowned upon that an individual have access to such a magnitude of PII, since an individual with no oversight or formalised accountability

may be perceived as tempted to use the information for his own personal gain. Although the functionality is currently not in place, the laws require that data subjects must have access to interact with the data available on them. With only a single individual processing these requests, he/she may soon have a backlog, and as a result, not adhere to the legislation anymore.

In all instances, the data subject needs to give express permission that PII may be made available. In none of the instances this would be adhered to, unless the system is further customised to only show and store PII that meets specific criteria, e.g. only phone numbers that belongs to a specific network. However, to facilitate this, the data will have to be cross-correlated with another database.

5.2 Reducing the Amount of PII Disclosures

A number of options to reduce the amount of PII being disclosed online have been identified; such as raising awareness, communicating with the affected parties and informing the privacy regulators.

Raising Awareness. One of the best ways to reduce the amount of PII being disclosed is to raise awareness regarding the leaked information as well as the requirements to be compliant with the PoPI Act [14]. Research shows that 91 % of successful data breaches rely on employees and customers falling victim to spear phishing and social engineering attacks [15]. This links strongly to ethical aspects in terms of personal information. PII may only be collected, used and disclosed with the knowledge and consent of the individual [16]. Although companies with an online presence have a responsibility towards their customers to protect their personal information, the customers should also be aware of the status and availability of their data. A customer can, for example, not sue a company for online PII disclosure if the customer himself inadvertently shares his personal information on Facebook.

In addition, awareness on data breaches can protect people from legal actions (individual as well as vicarious liability). It is a common assumption that most company data breaches can be attributed to technology and software vulnerabilities [15]. Awareness also enables people to identify possible breaches, for example if a person is contacted by an international company, the possibility exists that the PII was transferred across the country's border. To address this, additional measures can be implemented to limit the amount of system abuse by authorised users by implementing logging of all system accesses and putting in place a double authorisation system.

The use of the application in a legal and ethical manner may contribute to raising awareness since real life statistics on South African PII leakage can be made available. The benefit of raising awareness is that it assists in avoiding unfavourable publicity. In the business world, public reputation strongly influences the value assigned to its stock by shareholders. If a company is often linked to data breaches, customers will lose confidence in the company's ability to adequately protect their information.

Communicating with Affected Parties. While the way in which PII is leaked on the Internet differs from instance to instance, the cumulative results of disclosed data (as obtained by the developed system) provide a quantitative measurement indicator.

This measurement is useful to express the seriousness of the problem or to act as a baseline for future experimentation. As a starting point, the measurement indicator can be communicated to the website owners where the information resides. However, the website owners often only act as service providers and not the data custodians responsible for the data. South African privacy legislation dictates that the responsibility to safeguard personal information lies with the data custodian. The measurement indicator thus needs to be further communicated in order to make the data custodian aware of the transgressions. It is, however, not always an easy task to locate the data custodian.

Whether used by an individual, business or government department, an alternative approach is to notify the person whose personal information is being disclosed, with the intention that it becomes their responsibility to follow up on the removal of the leaked PII. This in itself may be a difficult task. The PII disclosed might be only an ID number without any additional information. In order to identify the affected person and obtain up-to-date contact information may require co-operation between more than one entity adding complexities to the potential solution. In addition, if an affected individual is notified, a link to the leaked data should be provided in order for the individual to follow up with the service provider on the removal thereof. However, in doing so, the PII of other affected parties will be further distributed. A solution to the identified difficulties would be to work in close partnership with law firms where the law firm could use the personal data being disclosed to force the service provider to take responsibility and notify the parties involved.

Informing the Regulator. The PoPI Act prescribes the establishment of a juristic person to be known as the Information Regulator, which will act independently and only be subjected to the Constitution and to the law. The overarching functions of the Regulator in terms of the PoPI Act are to promote an understanding and acceptance of the conditions for the lawful processing of personal information, provide education and monitor and enforce compliance to the PoPI Act [4]. At the time of writing, such a regulator was not yet put into place, but it is estimated to be established by middle 2016 [17].

The Regulator will be tasked with monitoring and enforcing compliance, supporting privacy related codes of conduct, handling complaints and facilitating cross-border cooperation in the enforcement of privacy laws [18]. As such, once operational, the Regulator will be responsible for addressing instances of breached data in South Africa. However, a concern in terms of informing the Regulator unless legally required is that it might raise unwanted questions on why this kind of data is collected and what methods were used to obtain this information. Collection could be perceived as Government interference or may raise spying concerns. Notification of leaked data might also lead to the assumption that it is the responsibility of the person who notified the third party to take action on the matter and to help remove the leaked information from the responsible websites. However, if the system is used by a government department in this case, there should not be an ethical concern.

6 Conclusion

Technology is becoming an integral part of life, and is often entwined with intimate, personal details. In recent years, the frequency of data breaches are increasing and the problem is that the data disclosed may be used for various criminal activities and cyber-attacks [19, 20]. Previous work examined the amount of PII publicly available at a stage in time when privacy and data breach legislation were introduced in South Africa. The Cyber Protect system that forms the basis of this paper is currently used as a research project, collecting leaked personal information online.

The purpose of the research project was to see if the amount of PII found online reduces over time, since the PoPI Act has been signed into law. The expectation was that the recently enacted South African privacy legislation would lead to a reduction in the amounts of PII being publicly disclosed. However, upon examination of the temporal data gathered from 2014 to 2015, only a slight improvement could be observed with the amounts of personal information being disclosed still substantial. One argument for the slow reduction in leaked information is that while the PoPI Act has been promulgated, it is not yet enforced. In addition, the South African privacy regulator is not yet appointed. There have thus been no formal charges and cases presented in a court of law against an individual or company that could spur greater public compliancy. This paper investigated the legal and ethical issues involved when using the system to pro-actively collect personal information being disclosed online. Although it is a research project, the system still needs to comply with the law and must be done in an ethical manner. It is argues that by using the system in an ethical and legal manner, it might be possible to reduce the amount of online PII disclosures.

As discussed, the user of the system has a potentially big impact on the ethical use of the system: it is generally accepted that government departments have access to personal information; businesses that are properly governed may also have access to personal information; however, an individual that are not accountable to a higher authority may potentially use the collected personal information for his own personal use. The PoPI Act is in line with similar International Acts, it could be beneficial to look at the legal and ethical implications that were involved in those Acts at the time of compliance and enforcement.

References

1. Shackleford, D.: When Breaches Happen: Top Five Questions to Prepare for. A SANS Whitepaper, SANS Institute, June 2012. http://www.sans.org/reading-room/whitepapers/analyst/breaches-happen-top-questions-prepare-35220. Accessed 3 June 2016
2. Rozenberg, Y.: Challenges in PII data protection. Comput. Fraud Secur. **2012**(6), 5–9 (2012)
3. Data breaches often not detected for months, report finds, Global Space (2013). https://www.globalscape.com/blog/2013/2/14/data-breaches-often-not-detected-for-months-report-finds. Accessed 12 Jan 2016
4. South African Government Gazette: Protection of Personal Information Act (2013). www.gov.za/documents/download.php?f=204368 . Accessed Nov 2014

5. Botha, J., Eloff, M., Swart, I.: Pro-active data breach detection: examining accuracy and applicability on personal information detected. In: Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, Boston (2016)
6. Romanosky, S., Telang, R., Acquisti, A.: Do data breach disclosure laws reduce identity theft? J. Policy Anal. Manag. **30**(2), 256–286 (2011)
7. Justice and Constitutional Development: Discussion of the Cybercrimes and Cybersecurity Bill, Republic of South Africa (2015). http://www.justice.gov.za/legislation/invitations/CyberCrimesDiscussionDocument2015.pdf. Accessed 11 Jan 2016
8. Reynolds, G.: Ethics in Information Technology: Thomson Learning, Canada (2003)
9. Noblet, T.: Business IT: Understanding Regulatory Compliance, (N.D.). https://technet.microsoft.com/en-us/magazine/2006.09.businessofit.aspx. Accessed 11 Jan 2016
10. Goodburn, D., Ngoye, M.: Privacy and the internet. In: Buys, R.-H., Cronjé, F. (eds.) Cyber-law @ SA II - the Law of the Internet in South Africa, 2nd edn, p. 171. Van Schaik Publishers, Pretoria (2004)
11. Botha, J., Eloff, M., Swart, I.: The effects of the PoPI Act on small and medium enterprises in South Africa. In: Information Security for South Africa (ISSA), Johannesburg (2015)
12. Wietryk, K.: Data Protection in the European Union and other Selected Countries: A New Comparative Study, (N.D.). http://www.kwr.at/fileadmin/res/pdf/publikationen/mag-arno-cichocki/10541_Data_Protection_Austria.pdf. Accessed Feb 2015
13. Hannes, B., Marius, A.: Information Ethics and the Law. Van Schaik Publishers, Pretoria (2012)
14. Botha, J., Eloff, M., Swart, I.: Evaluation of online resources on the implementation of the protection of personal information act in South Africa. In: Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS 2015, Kruger National Park (2015)
15. Pearson, A.: Protect Your Organization Against 91 % of Data Breaches (2015). http://blog.securityinnovation.com/blog/2015/11/protect-organization-against-91-percent-data-breaches.html. Accessed 15 Jan 2016
16. Office of the Information and Privacy Commissioner: Privacy-Proofing Your Retail Business - Tips for Protecting Customers' Personal Information. Canada (2007)
17. Michalsons: Information Regulator in South Africa (2015). http://www.michalsons.co.za/blog/information-regulator-in-south-africa/13893. Accessed 11 Jan 2016
18. Republic of South Africa: Protection of Personal Information Act (2013)
19. Paganini, P.: Cybercrime exploits Anthem data breach in Phishing campaigns (2015). http://securityaffairs.co/wordpress/33278/cyber-crime/anthem-phishing-campaigns.html. Accessed 14 Jan 2016
20. Zetter, K.: Hackers Finally Post Stolen Ashley Madison Data. http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/. Accessed 11 Jan 2016