The Protection Of Personal Information (POPI) Act - Impact On South Africa

Michelle de Bruyn, Stellenbosch University, South Africa

ABSTRACT

South Africa has received its own data protection legislation - the Protection of Personal Information (POPI) Act - in November 2013 and is expecting the government to appoint an Information Regulator to enforce the letter of the law. Until then, South African businesses will have time to get their house in order, but uncertainty exists as to how businesses will be affected when this happens. It is anticipated that the enforcement activities by the Information Regulator will be similar to how it is done by the Information Commissioners Office (ICO) in the United Kingdom. The ICO has been enforcing compliance with the Data Protection Act (DPA) of the United Kingdom since it obtained its enforcement powers in April 2010. This article summarises all actions taken by the ICO from April 2010 until the end of December 2013 to determine the industries most affected, the contraventions with the highest frequency and, where applicable, the highest monetary fines.

This article should provide some insight into what South African businesses can expect after the Information Regulator is appointed and starts to enforce the law. It will also enable them to focus their attention on the safeguarding of business areas with increased data protection risks as well as provide some counter measures that can be taken to prevent punishable contraventions.

Keywords: Privacy; Data Protection Act; POPI; Protection of Personal Information; Information Regulator; Information Commissioners Office; ICO

INTRODUCTION

The first privacy legislations were enacted in the early 1970's. The Data Protection Act of the West German Land of Hesse became law in 1970 and the Data Act of Sweden in 1973 (Clarke, 1989). Privacy legislation originally stemmed from the combined use of technology with information. The automated replication abilities of technology, like photocopying, microfilm and telecommunications, introduced the initial concerns about inappropriate or biased information practices (Clarke, 1989). Since the early 1970's, new technologies have been advancing at a rapid pace and, according to Greenleaf (2013b), 99 countries had enacted privacy laws and 21 countries had privacy bills by June 2013. This indicates a clear global trend in the adoption of privacy legislation (Greenleaf, 2013c:1).

Following this global trend, South Africa (SA) enacted its own privacy legislation - the Protection of Personal Information (POPI) Act on the 26th of November 2013 (POPI, 2013). The act protects the privacy rights determined by section 14 of the South African Constitution that specifies that "everyone has the right to privacy". The POPI Act will impact all responsible parties that collect, store, process and / or disseminate personal information as part of their business activities. A responsible party is defined by the POPI Act as "a 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". The act allows for certain exclusions which includes the processing of information in one's personal capacity, information that has been de-identified using anonymisation techniques (ICO, 2012e) or information that has been collected on behalf of a public body that promotes national security and public safety (POPI, 2013).

The POPI Act was based on a thorough investigation of global privacy laws by the South African Law Reform Commission (SALRC) that based the principles of the act mainly on those implemented by the Organisation for Economic Cooperation and Development (OECD) and the European Union (EU) (Heyink, 2011, p.2). SALRC recommended that, similar to the approach adopted by the EU, a body should be established to enforce, monitor and promote the adherence of the data protection act implemented (Heyink, 2011, p.8). As a result, the POPI Act prescribes that an Information Regulator must be appointed by the government to ensure the enforcement and promotion of the rights protected by it (POPI, 2013, p.17). In the United Kingdom (UK), the Information Commissioner is currently entrusted with the enforcement responsibilities in terms of the Data Protection Act (DPA). The effect of the POPI Act on South African companies remains to be seen, but because the legislation and method of enforcement is based on similar principles adopted by the DPA (De Stadler, 2013), it can be argued that South African entities can look towards the UK to predict what the impact of the POPI Act will be on South African entities (Tubbs, 2014).

According to Berry (2014, p.41), the new legislation will significantly impact the methods companies' use to gather, save, utilise and distribute personal information as specific requirements of the POPI Act will have to be complied with. A study was done by IQ Business, in conjunction with the South African Institute of Chartered Accountants, to test the South African companies' readiness for the new act. They found that company attitudes and procedures towards protecting the privacy of personal data needed attention and indicated that a lot of work still had to be done by these companies to become compliant with the letter of the law (IQ Business, 2014). They predict that, in addition to the civil and criminal actions that could be taken against non-complaint companies, the impact of possible reputational damage could be even more severe, and possibly detrimental, for a company's future (IQ Business, 2014, p.37). They also explored a possible advantage for companies to ensure compliance as it promotes the transparency in terms of what, how and where personal information is stored within companies (IQ Business, 2014, p.37).

The POPI Act includes data protection requirements that are similar to the DPA as well as guidelines in terms of appropriate direct marketing techniques (POPI, 2013) and adherence to it will be monitored and enforced by the Information Regulator. The UK has separate regulations - the Privacy and Electronic Communications Regulations (PECR) - which prescribes acceptable direct marketing techniques (PECR, 2003) and the enforcement thereof also rests within the powers of the ICO. Contraventions, in terms of PECR, have been included in this study because the content of the POPI Act represents the content of the combination of the DPA and PECR.

This study summarises the enforcement actions taken by the ICO in the UK to ascertain what contravening actions occurred most frequent and what industries were affected the most by the enforcement of the DPA and PECR by the ICO. This study attempts to use the results obtained by it to identify industries with higher data protection risks and to determine what contraventions led to the relevant enforcement actions taken by the ICO. The study also considers if the contraventions identified could have been avoided by the implementation of precautionary measures.

RESEARCH OBJECTIVE AND CONTRIBUTION

POPI has been promulgated on the 26th of November 2013 and South African businesses have time to implement processes and procedures internally to ensure that they comply with the requirements of the act. The businesses also need to minimise the risk of contravention of any stipulations of the act before the Information Regulator is appointed and receives its enforcement powers (POPI, 2013). Section 40 of the POPI Act determines that an Information Regulator will be appointed by the government and that it will be responsible for the education of South African businesses and public regarding their responsibilities and rights regarding the protection of private information. The Information Regulator will also be responsible for the monitoring and enforcement of adherence to the act, the handling of complaints in terms of privacy violations, the conducting of research and the issuing of codes of conducts, where required, as well as the facilitation of cross border cooperation between different countries in terms of different privacy laws (POPI, 2013).

According to sections 107 and 109 of the POPI act, it determines that the Information Regulator may impose a fine of up to R 10 million or imprisonment that does not exceed 10 years or a combination of a fine and

incarceration (POPI, 2013). The possible monetary fines and imprisonment with the additional prospect of reputational damage (IQ Business, 2014, p.37) pose a clear threat to South African businesses should they be found in breach of the requirements of the act. The purpose of this article is to identify the contravening actions that could be punishable by the Information Regulator as well as what industries are inherently exposed to higher levels of risk in terms of privacy and data protection. The article also aims to provide business leaders and IT managers with possible precautionary steps that can be implemented to avoid data protection breaches in terms of the POPI Act. The basis for the conclusions reached in this study will be drawn from the summaries made of the different enforcement actions taken by the ICO on DPA and PECR breaches. The summaries indicate the monetary value and frequency of the contravening actions that were punished by the ICO as well as the industries affected by it.

This article addresses the following research questions:

- What similarities exist between the Data Protection Act and the Privacy and Electronic Communications Regulations of the United Kingdom and the Protection of Personal Information Act of South Africa?
- What contraventions led to the enforcement actions taken by the Information Commissioners Office?
- Which industries were most affected by the enforcement actions taken by the Information Commissioners Office?
- What precautionary measures could have been implemented against the occurrence of the high frequency contraventions?

LITERATURE REVIEW

A literature review was done to determine what personal data and information is referred to in the context of data protection legislation and also why it is important to protect it. A comparison between the POPI Act of SA and the DPA and PECR of the UK were also done to establish differences and similarities in the conditions and principles rooted in both acts. This was done to affirm why it is appropriate to use the outcomes in the UK to predict what can be expected in SA in terms of the enforcement of the POPI Act. The different enforcement types used in the UK are explained and the effects of possible reputational damage to companies are also discussed briefly.

What Is Personal Data And Information?

The POPI legislation defines personal data and information as any information that enables a user of the information to identify the data subject which could be a natural or juristic person (POPI, 2013, p.14). It includes information regarding race, marital status, health, gender, sex, pregnancy, ethnic origin, religion, disability, belief, etc. (POPI, 2013, p.14), as well as any identifying number or symbol, like an e-mail address, physical address, telephone number or online identifier.

According to Greenleaf (2013a, p.236), the legal definition of personal data poses two restrictions on the scope of data privacy laws. Firstly, they do not extend to data that does not identify a person but allows for personalised interaction with a specific person. Examples of this would include the use of software to enable behavioural marketing where companies use software to construct personal profiles, which excludes names or online identifiers but allows the gathering of a significant amount of details about individuals (Schwartz & Solove, 2011, p.1818). In section one of the POPI Act, "online identifiers" are included in the "personal information" definitions and the ICO has provided guidelines on the use of cookies - a file downloaded from websites enabling a website to recognise specific devices - in the UK (ICO, 2012f) to assist in addressing this restriction.

The second restriction is posed on the exclusion of data that is stored in a non-transitory form, like some forms of closed circuit television (CCTV) recordings (Greenleaf, 2013a, p.236). The ICO provides a CCTV code of practice (ICO, 2008) that includes guidance on how and where the recorded material must be stored in a responsible manner. The POPI Act does not address this concern directly (POPI, 2013), but the future Information Regulator will also be able to provide guidance to South African businesses about the preferred business practises to be employed regarding these types of material.

Importance Of Data Privacy Protection

The exponential advances in technology are increasing the ability of organisations to accumulate, store, process and disseminate personal data (Greenleaf, 2013a, p.221). People use their computers and mobile phones nearly every day, inadvertently leaving comprehensive digital footprints behind. Our electronic devices are enabling enormous amounts of personal data to be moved via the internet between different jurisdictions without our knowledge (Greenleaf, 2013a, p.221), and electronic sensors, like CCTV cameras and other biometric identifiers, are being used extensively in our work and living environments (Greenleaf, 2013a, p.221). Data mining companies use special software to identify patterns in personal data obtained via various means and from various sources to predict people's behaviour in the future based on their past actions (Greenleaf, 2013a, p.221). Cloud computing is being used more frequently by businesses to acquire advanced processing power and storage capacities at reduced costs as a result of the benefits of economies of scale (Basson, 2014, p.10). This exposes businesses to privacy risks if the hosting country's legislation does not meet the minimum data privacy requirements prescribed by legislation of the responsible party's country (Basson, 2014).

The internet has made the international market very small with the transference of data, in most cases, being only a mouse click away. It is important to recognise that no prevailing organisations exist that govern data privacy over the internet globally (Greenleaf, 2013a, p.222). According to Greenleaf (2013a, p.222), "privacy" is a broader term than "data privacy" and includes the right to not being observed, the right to solitude, and the right to the protection of bodily integrity, but these meanings overlap because of ubiquitous data collection. Greenleaf (2013a, p.222) states that data privacy laws are the legal instrument that is the most capable of protecting privacy in this context, but it does not diminish other legislation that protects individual's rights as well. The impact on privacy of these other legislations, e.g. consumer protection laws and constitutional rights, falls outside the scope of this article and will therefore not be explored further.

According to Greenleaf (2013a, p.224-225), data privacy laws can only be effective if they include a comprehensive set of data privacy principles that agrees with international standards, like the OECD guidelines, and it must have a mandatory legal enforcement mechanism (Greenleaf, 2013a, p.224-225). It should also cover most of a country's private and public sectors and not only be focused on a few subsectors, like "credit reporting" or "health" (Greenleaf, 2013a, p.225). Greenleaf (2013a, p.225) recommends that an independent "data protection authority" must be established to ensure the enforcement of the law, perform investigations of privacy complaints received and be involved with the improvement and amendments of privacy legislation.

Comparisons Between The POPI Act Of SA And The DPA And PECR Of The UK

The POPI Act and the DPA both use the term "data subject" when referring to the subject of the personal data or information (DPA, 1998; POPI, 2013). The enforcement body of the UK is called the Information Commissioner and the equivalent South African body that must still be appointed will be called the Information Regulator (DPA, 1998; POPI, 2013). The POPI Act uses the term "responsible party" when referring to the person or entity that "determines the purpose of and means for the processing of personal data and information" (POPI, 2013) and the DPA refers to a "data controller". Both acts define a separate subset of personal data referring to information that is deemed more sensitive in nature, like that which relates to a data subject's racial or ethnic origin, political views, religious convictions and the membership of trade unions (DPA, 1998; POPI, 2013). Information about a data subject's sexual preference and information about any criminal convictions are also deemed to fall within this sensitive data category (DPA, 1998; POPI, 2013). The term used in the POPI Act to describe this subset of personal information is "special personal information" and the term used by the DPA for the same subset of information is "sensitive personal information". In both the POPI Act and DPA, more stringent conditions for protection of data exist when a responsible party or data controller collects, uses, stores, disseminates or distributes data or information of this sensitive nature (DPA, 1998; POPI, 2013).

The DPA requires data controllers to register as such with the ICO if they perform any pertinent data collection functions as part of their business activities (DPA, 1998) and the POPI Act does not have such a requirement (POPI, 2013) where responsible parties only process general personal data and the data subject has been adequately notified. According to section 57 of the POPI Act, prior approval must be obtained from the Information

Regulator under certain circumstances, which includes the linking of information of data subjects obtained by different sources, the processing of information on criminal behaviour, as well as information on credit reporting. Although not all responsible parties will be required to register with the Information Regulator, it is not expected that the enforcement of the act will be less effective as the embedded conditions of the POPI Act will still apply to all responsible parties. The enforcement of both the DPA and the POPI Act originates or will originate from the resolution of complaints received by the data protection agency from various organisations or members of the public (DPA, 1998; POPI, 2013).

According to Greenleaf (2013a, p.237), the ten common core data privacy principles that should be included in privacy legislation so that it can be effective are: 1) fair data collection, 2) data quality, 3) purpose specification, 4) purpose notification when data are collected, 5) limitation to specified data uses, 6) reasonable security safeguards, 7) openness, 8) access and correction of an individual's data, 9) accountability of the responsible parties, and 10) implementation or instruction of data export restrictions. These core principles are listed and described briefly in Table 1 with specific references to where these conditions are addressed in the relevant acts.

The principle of "openness", in terms of data practices, is included as a core data privacy principle by Greenleaf (2013a, p.237) but is not included in the principles of the DPA. Condition 6 of the POPI Act refers to the openness requirement but then defers the enforcement of this practice to the Promotion of Access to Information Act. Both SA and the UK have separate legislation that enforces this core principle and therefore falls outside the scope of this article. The respective acts that protect the "openness" principle are the Promotion of Access to Information Act in SA and the Freedom of Information Act in the UK and will not be explored further in this study.

Table 1: Comparison Of Core Data Privacy Principles Between The POPI Act And The DPA

No.	Core Principle	POPI (RSA)	DPA (UK)
1	*Collection*: Private data collection may only be done in ways that is fair, lawful and with the knowledge and consent of the data subject.	Condition 2	Principle 1
2	*Data quality*: Private data collected must be accurate and relevant.	Condition 5	Principle 4
3	*Purpose specification*: Private data may only be collected for a specific use and the purpose must be specified at collection time.	Condition 3	Principle 2
4	*Purpose and rights notification*: Data subjects must be notified that their data will be collected and for what purpose it will be used.	Condition 3	Principle 2
5	*Uses*: The personal data may only be used or processed for the purposes that the data was originally collected, i.e. excessive processing is prohibited.	Condition 4	Principle 3 Principle 5
6	*Reasonable security safeguards*: The necessary technical and procedural practices should be implemented to ensure the safety of the personal data.	Condition 7	Principle 7
7	*Individual's access and correction*: Data subjects have the right to know what information on them is stored and processed by the responsible party / data controller. The responsible party / data controller have a responsibility to affect any corrections if the data subjects inform them thereof.	Condition 8	Section 7
8	*Accountability*: It is the obligation of the responsible party / data controller to implement and monitor adherence to the conditions of the act.	Condition 1	Principle 6
9	*Data export restrictions*: Data transfers to countries may only be done to countries that have adequate data privacy legislations in place.	Chapter 9, Section 72	Principle 8

(Adapted from DPA, 1998; Greenleaf, 2013a; POPI, 2013)

Nine out of the ten (90%) core principles, that should be incorporated in data privacy legislation to be effective (Greenleaf, 2013a), form part of the POPI Act and the DPA. It is apparent from Table 1 that the core principles on which both of the acts are based are significantly similar. It could therefore be deduced that it is reasonable to expect the enforcement of both acts will lead to similar outcomes. This notion is supported by De Stadler (2013) and Tubbs (2014) and it is from this expectation that the summaries of all the enforcement actions taken by the ICO in the period under review were created.

The PECR of the UK protects individuals' rights in terms of unsolicited direct marketing techniques and the ICO has provided detailed guidance to businesses in terms of what is acceptable direct marketing behaviour (ICO, 2013c). This guidance document determines that direct marketing may only happen in the following instances:

- Expressed permission should be obtained from the targeted people in the specific marketing campaigns. Records must be kept of where and how these permissions were obtained.
- The direct marketing standard operating procedures should be tailored per marketing attempt as the consent obtained varies per marketing initiative, e.g. there are more stringent rules in terms of marketing calls than mail marketing.
- Direct marketing via calls, texts or e-mails will probably not be valid if it is made to persons from details obtained from a third party. If a company wants to use data obtained from third parties, the data will have to undergo thorough testing to ensure that the correct permissions were obtained from the relevant data subjects before it can be used.
- Marketing phone calls may only be made to data subjects that are not registered with the Telephone Preference Service (TPS) of the UK. No marketing calls may be done to data subjects that are registered with the TPS unless specific prior consent has been received by the specific data subject.
- No recordings may be made of marketing calls without the prior consent of the data subject.
- No marketing texts or emails may be sent to data subjects without expressed prior approval. Marketing to data subjects that are clients of the company may be allowed in certain circumstances.
- Vendors must immediately stop direct marketing to any data subject that has indicated they want to "opt out".

In chapter eight of the POPI Act, it states that no electronic direct marketing via text may be done to any data subjects without the expressed permission obtained to do so. Companies must provide data subjects the option to opt out of direct marketing drives and affect their request to exclude them from these drives immediately. Companies are allowed to market their products to clients if the products are similar to the products sold to them previously, but the data subject must be enabled to stop the receivables of such marketing at any time and with immediate effect.

In essence, the requirements of the POPI act corresponds with the requirements specified in the guidelines provided by the ICO listed above. It is therefore expected that transgressions in terms of the above guidelines would possibly also construe a punishable offence in South Africa. The membership of data subjects to the TPS is not dealt with in the POPI Act, although South African data subjects can currently register with the Direct Marketing Association of SA's (DMASA) "Opt Out" database to stop unsolicited contact from vendors, but adherence to this initiative is voluntary and only required from DMASA members. The public will have to wait and see whether or not the Information Regulator determines that the DMASA's "Opt Out" database will be used in the same fashion as in the UK by South African companies, but it is clear that unsolicited direct marketing will not be tolerated.

Types Of Enforcement Actions

The ICO can impose monetary penalties, enforcement notices, judgements and prosecutions if a contravention of the DPA or the PECR was confirmed. The ICO has determined certain guidelines to indicate which contravention will fit into which type of action (ICO, n.d.-c) and the guidelines are briefly discussed below.

Monetary Penalties

According to the Section 55A of the DPA, the ICO can impose a monetary penalty notice of up to £500 000 if a serious contravention of the data protection principles has occurred that was likely to cause substantial damage or distress and the data controller knew or should have been aware of the risk and did not impose reasonable steps to prevent it. The ICO (2013e) provides guidance on how the monetary penalty should be calculated or determined and takes into consideration the seriousness of the offence, whether there were any mitigating or aggravating factors as well as the financial position of the data controller. The guidance provided by the ICO (2013e) stipulates that the

monetary penalties should be enforced in a consistent manner and it should be reasonable in terms of the violation that has occurred.

Sony Computer Entertainment Europe Limited was fined with a monetary penalty (ICO, 2013k) when the Sony PlayStation network platform came under attack via several distributed Denial of Service attacks and personal data stored on the platform was accessed by the attacker. The data accessed included customer names, email addresses, birth dates and passwords. Millions of customers also entered their encrypted credit card details, but there was no evidence that this information was accessed. The ICO found that the network platform did not meet the standards of new technical developments and as a result was inappropriate at the time of the attack. The ICO was satisfied that this breach was a serious offence and that a contravention of this sort could have caused substantial damage or distress and, as a result, decided on the significant fine of £250 00.

Enforcement Notices

The ICO can also impose an enforcement notice that forces an organisation to stop or change their internal processes or actions so that they will not be acting in contravention with the DPA (ICO, 2014d). An example of this is where the ICO imposed an enforcement notice on Google Inc. (ICO, 2013f) to securely destroy all personal information collected without permission through their street view vehicles. The vehicles were used to collect data in the aim of improving their geographic location database, but they also collected data that included e-mail addresses, URLs and passwords from open Wi-Fi networks.

Undertakings

Undertakings are issued by the ICO to organisations or persons that undertake to implement certain actions or processes to improve their compliance with the DPA (ICO, 2014g). Undertakings are signed by the ICO and the contravening organisation or person which then concludes an agreement between the two parties that the suggested changes have been agreed upon by both parties. Google Inc. and the ICO undersigned an undertaking where Google Inc. (ICO, 2010a) undertook to provide their employees with training in terms of data privacy principles and security awareness.

Prosecutions

The ICO can also prosecute criminal contraventions in terms of the DPA (ICO, 2014f). Prosecutions have been done for contraventions in terms of section 55 of the DPA which forbids the unlawful collection of personal data and section 17 of the DPA which requires data controllers to notify the ICO that they are data controllers. A former Barclays Bank employee was prosecuted and fined £3 360 after accessing customers' account details illegally (ICO, 2013a). She acquired information regarding the number of children a customer had and passed the information on to a friend of her who was in a relationship with the said customer at the time.

Enforcement Actions In Terms Of POPI

According to chapter 11 of the POPI Act, the Information Regulator will also be able to impose monetary fines to the maximum value of R10 mil each and enforcement notices (POPI 2013, p.92) to instruct companies to stop from continuing with inappropriate data practises. The Information Regulator will also be able to instruct businesses to take specified prescribed steps (POPI 2013, p.92) resembling the use of undertakings by the ICO. The risk for a criminal conviction by means of imprisonment in terms of the POPI Act cannot be measured in this study because the ICO does not have the power to impose imprisonment actions and, as a result, the possibility of enforceable imprisonment by the Information Regulator of SA falls outside the scope of this article. Despite the fact that the ICO does not have the right to send a convicted person to prison, a shortfall, according to the UK Justice Committee (2012) in the enforcement powers of the ICO, the enforcement rights and responsibilities of the ICO and the Information Regulator are similar. This supports the belief of De Stadler (2013) and Tubbs (2014) that SA can look to the UK to envisage how the Information Regulator will enforce its powers when the time comes. The Information Regulator will also have a right to publish decisions, findings and actions taken if it's believed that it will be in the public's interest to do so.

Reputational Damage

Additional to the enforcement actions and the associated potential monetary implication as discussed above, reputational damages (IQ Business, 2014; Tubbs, 2014) can also significantly impact businesses if a judgment of non-compliance in terms of the privacy legislation is published by the data protection authority. An example of a company that faced reputational damage in the UK, as a result of a major security breach, is Sony Computer Entertainment Europe Limited when they were found guilty for a security breach that compromised the Sony PlayStation Platform when it was hacked in April 2011. Magee (2011) found that 94% of the UK public believed that this breach was damaging to Sony's reputation and it contributed to 77% of consumers being more cautious in providing their personal information on the internet.

The risk of reputational damage cannot be quantified, but it is expected that it could lead to a loss of future business and clients. International business opportunities can also be jeopardised if it is believed that the data security principles applied within a specific business are inadequate.

RESEARCH DESIGN AND METHOD

The literature confirms the importance of protecting businesses from the possibility of non-compliance with data protection legislation. Enforcement actions by data protection authorities can lead to significant monetary penalties, possible incarceration and also the potential of harmful and possible detrimental reputational damage. The literature confirms why South African companies can obtain valuable insights into possible data protection risk areas while they aim to protect the private information that they are responsible for. Summaries were made of all the enforcement actions taken by the ICO from the time when the ICO obtained its mandate in April 2010 until the end of December 2013 in order to understand how the ICO enforced the law. The different types of enforcement actions that the ICO used to administer its powers were by imposing monetary penalties, undertakings, prosecutions - that excludes incarceration - **and** by the application of enforcement notices.

Data Collection

The source data of the different summaries were collected from the ICO's website. For the summaries of the monetary penalties (ICO, 2014e), undertakings (ICO, 2014g) and enforcement notices (ICO, 2014d), access to the electronic copies of the physical documents issued by the ICO were obtained. The prosecutions summary (ICO, 2014f) was dependant on news reports as the ICO's official documentation, in this regard, was not available on their website or on the internet. Data pertaining to the enforcement actions before 2012 had been removed on the ICO's website at the beginning of 2014, but electronic copies were made by the researcher of all the documents used in the creation of the summaries and can be contacted if any queries arise. Most of this information can still be obtained from the Breach Watch website (ICO, 2014c) which provides information on UK regulatory breaches and activities.

Contraventions were classified per industry to identify if there are industries with higher data protection risks than others. The contraventions were also classified per contravening action to identify what the violations were with the highest frequency.

LIMITATIONS OF THE STUDY

- The study only looks at enforcements made by the ICO on contraventions of the UK DPA and PECR as these are the two acts that correspond with the implications of the POPI Act on South African entities. The ICO can also make judgements in terms of the UK Freedom of Information Act, Environmental Information Regulations and Infrastructure for Spatial Information in the European Community Regulations (ICO, 2011g), but this falls outside the scope of this article and enforcement actions relating to these acts have been excluded in the summaries for the sake of this study.
- Where an entity performed duties that overlapped with more than one industry, a decision was made on what the entity's main industry was, and only that industry was listed in the summary. There were minimal instances where this was done and it is not expected that the alternative selection would have a significant impact on the outcome of the study.

- The completeness of the summaries is dependent on the data availability in the public domain, the ICO's website and on the internet. If the ICO chose not to disclose or publish any actions taken by them, those actions would not have been included in the summaries. This could negatively impact the completeness of the data used to create the summaries presented in this study, but it is believed that the ICO would have published all the enforcement actions taken by them as it is their policy (Fox, Gorrill, Webb & Parker, 2010, p.3) to publish enforcement actions to enhance their reputation as "the authoritative arbiter of information rights, an educator and an influencer".

EMPERICAL RESEARCH FINDINGS

Enforcement Profile

Objective Of The Analysis

The total enforcements made by the ICO since April 2010 was summarised per enforcement type and per year and is presented in Table 2. The objective of this part of the analysis is to identify which enforcement type was used most frequently.

Findings And Deductions

Table 2: Number Of Enforcement Actions Implemented By The ICO For The Period April 2010 To 31 December 2013

Enforcement Type	2010	2011	2012	2013	Total	%
Monetary Penalty	2	7	25	18	52	23.64
Enforcement Notices	0	1	4	6	11	5.00
Undertakings	0	71	31	28	130	59.09
Prosecutions	0	10	9	8	27	12.27
					220	**100**

The most frequent action taken by the ICO was by means of agreed undertakings (59%) and imposed monetary penalties (24%). The frequency of the undertakings declined, while the imposed monetary penalties increased over the years under review, with 2012 having the highest number of issued monetary penalties to date. The reason for the initial high amount of undertakings in 2011 (71) and the gradual decline is due to the fact that the ICO started their enforcement regime by using undertakings as a precursor to more formal or harsh action in an attempt to motivate organisations to become compliant with the DPA (ICO, 2011g).

Monetary Penalties By Contravention

Objective Of The Analysis

The monetary penalties were summarised and the total, average, maximum, minimum amounts, as well as the number of violations per contravening action, are displayed in Table 3. The summary is sorted in descending order, with the highest average monetary penalty at the top.

Findings And Deductions

All the monetary penalties were issued in terms of sensitive personal information breaches, except for one that occurred in 2013 where a bank sent multiple faxes containing personal information - that was not deemed sensitive - to wrong recipients. The bank received a monetary penalty of £75 000 and it is included in the results of Table 3 under contravention nr 15: "Private information faxed to wrong recipient/s".

Table 3: Monetary Penalties Per Contravening Action

Nr	Contravening Action	Ave (£)	Total (£)	Max (£)	Min (£)	Number
1	Insecure disposal of hard drives containing personal data led to disclosure of sensitive personal information.	262 500	525 000	325 000	200 000	2
2	Sensitive personal information compromised due to attack on network. Controls implemented by data controller found to be inadequate.	250 000	250 000	250 000	250 000	1
3	Insecure storage of sensitive private information on paper records.	225 000	225 000	225 000	225 000	1
4	Direct marketing: Sending of unsolicited text messages	205 000	615 000	300 000	140 000	3
5	Insecure disposal of paper records containing sensitive personal information.	175 000	350 000	250 000	100 000	2
6	Sensitive personal data exposed in error on website.	175 000	175 000	175 000	175 000	1
7	Unencrypted back-up tapes lost.	150 000	150 000	150 000	150 000	1
8	Unencrypted DVD lost.	150 000	150 000	150 000	150 000	1
9	Unencrypted USB's stolen/lost.	115 000	230 000	150 000	80 000	2
10	Sensitive private information e-mailed to wrong recipient/s.	95 714	670 000	140 000	60 000	7
11	Unencrypted laptop/s stolen.	90 000	360 000	150 000	60 000	4
12	Direct marketing: Making unsolicited phone calls.	90 000	360 000	125 000	45 000	4
13	Hard copy of sensitive private information was provided/disclosed/sent to wrong recipient/s.	86 500	865 000	140 000	50 000	10
14	Sensitive private information unknowingly loaded onto internet.	85 000	170 000	100 000	70 000	2
15	Private information faxed to wrong recipient/s.	80 000	320 000	100 000	55 000	4
16	Hard copy of sensitive private information was lost / stolen.	77 500	310 000	100 000	70 000	4
17	Hard copy of sensitive private information was lost and leaked to media.	70 000	70 000	70 000	70 000	1
18	Unencrypted hard drive stolen.	5 000	5 000	5 000	5 000	1
19	Sensitive personal data exposed due to inadequate web hosting security.	1 000	1 000	1 000	1 000	1
	TOTALS	**111 558**	**5 801 000**	**325 000**	**1 000**	**52**

The four contravening actions that had an average monetary penalty in excess of £200 000 were the insecure disposal of hard drives, inadequate network security, inadequate control over the storage of paper records, as well as the sending of unsolicited text messages. There were two incidents relating to the insecure disposal of hard drives which led to the highest average (£262 500) and maximum (£325 000) monetary penalty being awarded, although this contravention could have been completely avoided (ICO, 2012c, ICO, 2012j, ICO, 2013j). Companies that need to replace old electronic equipment, especially that which stores personal data, must follow reasonable steps to ensure proper removal and/or deletion of personal data stored on the devices. When the disposal of electronic equipment is proposed within a company, the ICO's guidance document called "IT asset disposal for organisations" (ICO, 2012j) can be consulted.

One privacy breach occurred due to inadequate network security and led to a penalty of £250 000 (ICO, 2013k) and, according to the ICO, this breach could have been avoided if the company installed up-to-date software (ICO, 2013l). One fine was also issued for the insecure storage of paper records and led to a monetary penalty of £225 000 being issued (ICO, 2012b). This fine could have been prevented if proper physical access controls were implemented to safeguard the documents against unauthorised access. Three monetary penalties were awarded towards inappropriate direct marketing techniques used in the form of unsolicited text messages, with the average penalty being £205 000 and the maximum penalty being £300 000. There were also four monetary penalties issued in terms of unsolicited marketing phone calls, with an average monetary penalty of £90 000 and a maximum penalty of £125 000. These fines could have been avoided if the contravening companies adhered to the ICO guidelines (ICO, 2013c) on direct marketing which clearly states that no marketing may be directed at anyone without obtaining specific consent from them and also not to people who registered themselves at the TPS.

The only other contravention with a maximum penalty exceeding £200 000 was where paper records were insecurely disposed of (ICO, 2012m). The company received a penalty of £250 000 for discarding documents containing sensitive personal information at a paper recycling bank (ICO, 2012m) instead of shredding the documents and disposing of them securely. Another penalty that would have been close to the value of £200 000 was where personal data were exposed online due to incorrect web hosting security, but the penalty was reduced to £1 000 because the data controller was not trading at the time when the fine was issued (ICO, 2011f). In this instance, the offender did not consult an IT professional when the business IT system was created and a web-hosting service - which was intended for domestic use - was implemented that led to the compromise of sensitive personal information of about 6,000 data subjects (ICO, 2011f).

The contraventions that happened most frequently were the disclosure of sensitive personal information via paper documents (10 instances) with sensitive private information being e-mailed to incorrect recipients occurring seven times. Proper employee training and the implementation of appropriate internal processes could have mitigated or even have prevented these contraventions (ICO, 2012k, ICO 2013i).

Monetary Penalties By Industry

Objective Of The Analysis

A summary was made of the total, average, maximum, minimum amounts and the number of contraventions per industry to identify the industry that was most affected by the monetary penalties imposed. The summary is sorted in descending order, with the highest average monetary penalty at the top and can be found in Table 4.

Findings And Deductions

All the monetary penalties issued were in terms of sensitive personal information breaches except for one contravention which was made in 2013 by a bank that sent multiple faxes containing non-sensitive personal information to the wrong recipients. The bank received a penalty of £75 000 which is included in Table 4 under industry nr 10 - "Financial Services".

Table 4: Monetary Penalties Per Industry

Nr	Industry	Ave (£)	Total (£)	Max (£)	Min (£)	Number
1	Technology - Entertainment	250 000	250 000	250 000	250 000	1
2	Marketing	220 000	440 000	300 000	140 000	2
3	Health	145 000	1 450 000	325 000	55 000	10
4	Justice	140 000	140 000	140 000	140 000	1
5	Unspecified / Various Council Services	123 333	740 000	250 000	70 000	6
6	Police	100 000	300 000	150 000	70 000	3
7	Manufacturing	90 000	90 000	90 000	90 000	1
8	Social services	89 706	1 525 000	140 000	60 000	17
9	Energy Services	85 000	170 000	125 000	45 000	2
10	Financial Services	92 500	555 000	175 000	5 000	6
11	Education	70 000	140 000	80 000	60 000	2
12	Legal Services	1 000	1 000	1 000	1 000	1
	TOTALS	**111 558**	**5 801 000**	**325 000**	**1 000**	**52**

The four industries that had average penalties exceeding £140 000 were technology (£250 000), marketing (£220 000), health (£145 000) and justice (£140 000). The four industries that had a maximum penalty that exceeded £200 000 were health services (£325 000), marketing (£300 000), technology (£250 000) and unspecified council services (£250 000). It should be noted that the contraventions in the marketing industry were both for inappropriate direct marketing techniques (calls and text messages) and also that the penalty for legal services was suggested to be £200 000 but was reduced because the business was not operating at the time the penalty was awarded (ICO, 2011f).

The three industries that had incident rates exceeding 10 incidents per industry and represents 64% of the total monetary penalties issued were social services (17 incidents), health services (10 incidents), and unspecified council services (6 incidents). All of these services are provided by the local government of the UK (ICO, 2014b). Health and social services manage high levels of sensitive personal information and could attribute to the fact that these services attract a higher data protection risk and possibly harsher penalties, like monetary fines. Financial services had an incident rate of 6, which is the same as for unspecified council services.

Monetary Penalties Per Year

Objective Of The Analysis

A summary of the total, average, maximum and minimum amounts of penalties per year was made to identify if there was any trend over the years in terms of the monetary penalties issued.

Findings And Deductions

The monetary penalties issued by the ICO in terms of DPA and PECR for the period April 2010 to December 2013 are summarised in Table 5.

Table 5: Monetary Penalties Per Year For The Period April 2010 To December 2013

Description	2010	2011	2012	2013	Total
Penalties in £	160 000	541 000	3 120 000	1 980 000	5 801 000
Penalties in %	2.76%	9.33%	53.78%	34.13%	100.00
Average in £	80 000	77 286	124 800	110 000	111 558
Maximum in £	100 000	130 000	325 000	250 000	325 000
Minimum in £	60 000	1 000	50 000	5 000	1 000

The total amount of penalties imposed by the ICO for the period April 2010 to December 2013 is £5 801 000, with more than half of the monetary value being imposed in 2012 (54%, £3 120 000) and 34% (£1 980 000) being imposed in 2013. The significant increase in 2012 can be ascribed to the fact that the ICO has increased the use of monetary penalties to enforce compliance with legislation (ICO 2012h, p.30; ICO, 2013h, p.32). The decrease in 2013 could not be confirmed with a published strategic change by the ICO but could be ascribed to an increased awareness of data protection principles in UK organisations due to the continuous efforts of the ICO to communicate and publish the enforcement actions imposed since April 2010. The ICO does this to enhance businesses and the public's awareness of their data protection and privacy rights and obligations. This trend can be revisited in future studies to see if the monetary penalties enforced continue to decline in future years. The average (£124 800) and maximum (£325 000) penalties for 2012 is the highest since 2010 and is followed by the second highest average (£110 000) and maximum (£250 000) penalties in 2013.

Undertakings By Contravention

Objective Of The Analysis

A summary was made of the number of undertakings issued by the ICO in terms of the DPA and PECR since April 2010. The undertakings were divided into contraventions of personal information breaches and also where this personal information was deemed "sensitive". The summary can be found in Table 6 and is sorted with the contravening actions with the highest frequency at the top in descending order.

Findings And Deductions

Undertakings issued by the ICO is an agreement between the ICO and the entity where the entity commits to making specific improvements in their organisation to ensure adherence to DPA and PECR or to allow the ICO to conduct an audit (ICO 2011g, p.40). The ICO has most frequently made use of undertakings (refer Table 1) to ensure and implement compliance in terms of the DPA and PECR. Although undertakings do not have a financial

impact, the ICO publishes these undertakings (Fox *et al*., 2010) on their website and could lead to causal reputational damages. Undertakings could therefore be seen as a lighter (ICO 2012h) form of enforcement but should not be ignored because of the possible resultant reputational damage (Cetinkaya, 2013, p.7; ICO, 2014a).

A total number of 130 (refer Table 1) undertakings was issued by the ICO in the period under review, but some of them addressed more than one contravening action. Instances were identified where one undertaking was issued for more than one contravening action and it was included separately in the following summaries (Tables 6 and 7). This is the reason for the discrepancy between the number of undertakings in Table 1 (130) and Table 6 (144). The number of occurrences per contravening action, as well as the ratio of non-sensitive personal information versus sensitive personal information breaches, is shown. The follow-up undertakings are also indicated separately (refer Table 6) but were only implemented from 2013 (ICO, 2013h, p.34) to ensure that the improvements, agreed upon previously by means of an undertaking, have been implemented.

Table 6: Undertakings Per Contravening Action

Nr	Contravening Action	Number	Sensitive	Not Sensitive	Follow Up
1	Hard copy of private information was lost / stolen.	33	25	8	0
2	Unencrypted computer drive / laptop/s stolen.	21	14	7	0
3	Hard copy of private information was provided/disclosed/sent to wrong or unauthorised recipient/s.	13	10	3	0
4	Private information e-mailed to wrong recipient/s.	13	10	3	0
5	Unencrypted USB's stolen/lost.	11	7	4	0
6	Insecure disposal of paper records containing personal information.	6	6	0	0
7	Private information faxed to wrong recipient/s.	6	5	1	0
8	Inadequate website security provides access to personal information.	6	3	3	0
9	Disclosing personal information on website/internet.	4	2	2	0
10	Inadequate policies regarding maintenance, processing and storage of personal information.	3	2	1	0
11	Insecure disposal of hard drives / laptops containing personal data.	2	1	1	0
12	Personal Information compromised due to attack on network. Controls implemented by data controller found to be inadequate.	2	1	1	0
13	Sensitive private information unknowingly loaded onto internet.	2	1	1	0
14	Unencrypted CD / Back-up tapes lost.	2	1	1	0
15	Illegally obtaining personal information (without data subject's approval).	1	1	0	0
16	E-mail account hacked and personal information accessed due to inappropriate security measures and inadequate privacy policies.	1	1	0	0
17	Hard copy of private information was discarded insecurely.	1	1	0	0
18	Inadequate technical security and policies to safeguard data from unauthorised access within the organisation.	1	1	0	0
19	Insecure handling and storing of hard copy data.	1	1	0	0
20	Insecure website provides access to personal information.	1	1	0	0
21	Recorded information is inaccurate.	1	1	0	0
22	Storing of excessive information.	1	1	0	0
23	Third party personal data disclosed in response to "subject access request".	1	1	0	0
24	Failure to provide information within 40 days after "data subject request" was received.	1	0	1	0

(Table 6 continued)

25	Inadequate technical security and policies in terms of personal data collected with CCTV cameras as well as insecure distribution and storage.	1	0	1	0
26	Sending text messages to individuals without checking whether they had given their consent to be contacted.	1	0	1	0
27	Unauthorised transfer / disclosure of electronic personal information to a third party.	1	0	1	0
28	Unencrypted USB drive that is used to store personal information issued and used by staff	1	0	1	0
29	Follow up.	6	0	0	6
	Total	**144**	**97**	**41**	**6**

The contravening actions that exceeded 10 incidents were where paper records were lost or stolen (33 incidents), the theft or loss of unencrypted laptops (21 incidents), paper records being sent/disclosed or provided to unauthorised/wrong person/s (13 incidents), private information sent to wrong e-mail addresses (13 incidents), and unencrypted USB drives that were lost or stolen (11 incidents). Of the total (144) undertakings enforced, 67% of the contraventions represent sensitive personal information breaches and 29% the breach of personal information that was not sensitive. Follow-up visits by the ICO represent 4% of the undertakings issued.

The loss of paper records includes instances where employees took paper records home to perform work with it after hours and the records were lost or stolen before they could be returned to the office the following day (ICO, 2011m; ICO, 2011q). It also includes paper records being misplaced or lost within offices (ICO, 2012i), records being lost during an office move due to inadequate record controls (ICO, 2011i), records being left in streets and in public places (ICO, 2011l), as well as the loss of records in archives (ICO, 2011c). Most of the records lost in this way (75%) represent the breach of sensitive private information. Although the loss of paper records does not seem completely avoidable due to the inherent possibility of human error, the ICO provides guidance in the various undertakings to address and reduce the risks involved to acceptable levels (ICO, 2014g).

The unencrypted laptops (ICO, 2011d) and USB's (ICO, 2011q) stolen or lost could have been avoided by ensuring that the devices were properly encrypted before they were used. It is important to note that access control via password does not imply a device is encrypted. The ICO advises that all portable and mobile devices that are used to send and store any form of personal information should be protected by using approved encryption software (ICO, 2012l). Encryption software uses embedded mathematical algorithms to encrypt and protect information and the software used should always be up to date and meet the required certification standards (ICO, 2012l). The majority of information compromised in this way (66%) was sensitive in nature.

Paper records provided/disclosed/sent to unauthorised/wrong persons includes instances where financial records were sent to the wrong recipients (ICO, 2011a) and where records of social workers were accidentally sent to wrong families (ICO, 2011o). It also includes the disclosure of excessive information in response to data access requests (ICO, 2013d), as well as paper records being sent to wrong recipients after printer mix-ups (ICO, 2012d) occurred. These contraventions could probably have been avoided if the relevant personnel were properly trained in terms of data protection principles and if they performed additional checks to ensure the correct information was sent to the right recipients. Another breach that could have been avoided occurred when an employee placed records containing sensitive personal information in her car in such a manner so that the information on the records was clearly visible to people passing the vehicle (ICO, 2011h). The ICO has provided clear instructions in the relevant undertakings on how the risks of data protection breaches should be reduced to an acceptable level (ICO, 2014g). The instructions include that staff that works with or has access to personal or sensitive personal information should have proper training on the importance, methods and policies implemented by the entity to ensure proper protection of all private information (ICO, 2014g). Most of the data compromised (77%) in this section represented sensitive personal information.

E-mails sent to wrong recipients includes those where users entered or used wrong e-mail addresses, as well as the selection of wrong e-mail addresses from the auto suggested e-mail address in the e-mail software, which inadvertently led to the sending of private information to unintended recipients (ICO, 2011e). It also included an

incident where a Microsoft Excel file, with hidden personal data included in Pivot Tables, was sent to a recipient in response to a data request (ICO, 2011p). In a similar incident, the information was sent in response to a freedom of information request, but the Microsoft Excel spreadsheet that was used contained hidden columns which included personal information (ICO, 2012n). Another preventable breach of this nature occurred when an employee sent a pdf document containing the payslips of everyone employed in the specific company, to a previous employee in response to a payslip query (ICO, 2012g). The ICO provides guidance in the various undertakings to address or minimise the risk of exposing personal data by means of emails, and this includes staff training in the privacy policy of the company that could include the prohibition of the sending of private information via email (ICO 2011n ; ICO, 2014g). The information exposed in this manner was mainly (77%) sensitive personal information.

Undertakings Issued Per Industry

Objective Of The Analysis

Table 7 is a summary of the number of undertakings per industry to identify which industries were affected the most. It is sorted in descending order with the industry that had the highest incident rate at the top.

Findings And Deductions

The total undertakings summarised in Table 7 is 144. The reason for the discrepancy in the number of undertakings in Table 1 (130) with Table 7 (144) is explained in the above section. The follow-up undertakings are indicated separately.

Table 7: Undertakings Issued Per Industry

Nr	Industry	Number	Sensitive	Not Sensitive	Follow Up
1	Health services	38	34	2	2
2	Unspecified / Various Council Services	29	17	10	2
3	Social services	17	17	0	0
4	Education	15	8	7	0
5	Charity	7	5	1	1
6	Police	4	3	1	0
7	Legal services	3	2	1	0
8	Financial Services	3	1	2	0
9	Estate and/or Letting Agents	3	0	3	0
10	Court Services	2	2	0	0
11	Recruitment services	2	2	0	0
12	Recreational services	2	1	1	0
13	Food services	2	0	2	0
14	Housing	2	0	2	0
15	Union	2	1	0	1
16	Technology - Knowledge management	1	1	0	0
17	Chartered Institute	1	1	0	0
18	Pharmaceutical	1	1	0	0
19	Local Government Ombudsman	1	1	0	0
20	State for the Home Department	1	0	1	0
21	Technology - Online Monitoring Service	1	0	1	0
22	Cosmetics	1	0	1	0
23	Election services	1	0	1	0
24	Technology - Information	1	0	1	0
25	National Park	1	0	1	0
26	Media	1	0	1	0
27	Technology	1	0	1	0
28	Political organisation	1	0	1	0
	Total	**144**	**97**	**41**	**6**

The three industries that received the most and represents 58% of all the undertakings issued were health, council and social services, which all form part of the services provided by the UK local government. This high percentage rate corresponds with the findings in Table 4 where the same industries represented 65% of the total monetary value of penalties issued. From the above, it can be concluded that the health, council, and social services industries were affected most by the enforcement of the ICO's powers. The monetary penalties (100%) and undertakings (81%) issued for these industries mainly reflected data breaches that involved sensitive personal information. It could therefore be argued that the high level of sensitive personal information inherently managed by these industries - health details, religious convictions, and mental well-being - could have attributed to a higher exposure to data protection risks. The risks linked to these industries could have been minimised through the adoption, implementation, and training of staff on the data protection and health guidelines of the ICO (ICO, 2010b; ICO, 2014n.d.-e).

The percentage of undertakings issued in the education industry was 10% and similar to the undertakings for the social services industry (12%) but in contrast with the findings in Table 4 which indicated that only two monetary penalties of £70 000 each were imposed for this industry. The value of the monetary penalties issued in the education industry represents only 2% of the total value of monetary penalties. The undertakings in education represented an almost equal divide in terms of sensitive personal information (53%) and non-sensitive personal information (47%). The main contravening actions incurred in the education industry were for the loss of unencrypted laptops and/or other storage mediums (60%) and the loss of physical documents (20%) containing personal information. The opposing low value and number of imposed monetary penalties suggests that this industry does not necessarily pose an increased risk to data protection breaches, although educational institutions should ensure proper encryption of storage media and training for all staff on data protection obligations faced by the institutions in order to prevent any unnecessary contraventions.

Prosecutions Per Contravening Action And Industry Type

Objective Of The Analysis

The average, maximum and minimum penalty amounts per prosecution were summarised in Table 8 per contravening action and in Table 9 per industry to ascertain which contravening action and industry had the highest monetary fine and highest incident rate for prosecutions in terms of the DPA. No prosecutions were made in terms of PECR. Both tables were summarised in descending order, with the highest average monetary fine at the top.

Findings And Deductions

The only contraventions, in terms of the POPI Act, that could be expected to occur in SA (listed in Table 8) are where information was obtained and disclosed unlawfully as POPI does not require responsible parties to register as such with the Information Regulator. Contraventions in terms of section 17 of the DPA will therefore not apply to the South African context but is included in the summaries for the sake of completeness.

Table 8: Prosecutions Per Contravening Action

Contravening Action	Ave (£)	Total (£)	Max (£)	Min (£)	Nbr	Sensitive	Not Sensitive	Not Applicable/ Unknown
Unlawfully obtaining personal data (section 55).	6 099	97 590	45 000	614	16	7	9	0
Failure to notify ICO as data controller (section 17).	1 248	9 980	2 498	365	9	0	0	9
Unlawfully disclosing personal information.	420	420	420	420	1	0	1	0
Failure to notify ICO that they are using CCTV cameras.	365	365	365	365	1	0	1	0
Total	**4 168**	**108 355**	**45 000**	**365**	**27**	**7**	**11**	**9**

The average monetary fine for criminal offences is significantly lower £4 167 (0.037%) than the monetary penalties (£111 558) imposed for civil actions (refer to Tables 3 and 4). The contraventions with the highest total value (£97 590) and incident rate (16 incidents) were for convictions where personal data were obtained illegally, which will also be punishable in SA. The respective penalties of £45 000 and £28 700 were imposed on two separate employees that stole personal data from a telecommunications company and then sold it to third parties (ICO, 2011b) to be used for direct marketing purposes. These two penalties represent 90% of the total fines imposed through prosecutions and clearly represent an intentional act by the relevant culprits, which could have been avoided. The sensitive personal information breached in this section is insignificant (26%) compared to these types of breaches that led to monetary penalties (98%) and undertakings (67%).

Table 9: Prosecutions Per Industry

Industry	Ave (£)	Total (£)	Max (£)	Min (£)	No.	Sensitive	Not Sensitive	Not Applicable /Unknown
Telecommunications	36 850	73 700	45 000	28 700	2	0	2	0
Gambling	2 531	2 531	2 531	2 530	1	0	1	0
Direct marketing	2 498	4 995	2 498	2 497	2	0	0	2
Financial Services	1 911	11 467	3 360	1 180	6	1	3	2
Health Services	1 806	9 030	4 391	614	5	5	0	0
Estate and/or Letting Agents	731	5 847	1 056	365	8	1	3	4
Police Service	420	420	420	420	1	0	1	0
Restaurant and Bar Services	365	365	365	365	1	0	1	0
Private security	Unknown	Unknown	Unknown	Unknown	1	0	0	1
Total	**4 167**	**108 355**	**45 000**	**365**	**27**	**7**	**11**	**9**

It was identified that the ICO prosecuted a private investigator in the 2011 Annual Report (ICO, 2011g), but no other details could be confirmed on the ICO's website or from any other sources on the internet in this regard. It was decided to include the instance in the summary for the sake of completeness, even though the monetary value of the fine could not be confirmed. The industry that received the highest fines in this section was telecommunications, which was discussed in the above paragraph.

The industries that had the highest incident rate for information that was acquired unlawfully were health services (5 incidents), financial services (4 incidents), and estate and letting agents (4 incidents). The balance of the incidents, as indicated in Table 9 for the mentioned industries, was for not registering as a data controller with the ICO and will not be elaborated on further as this requirement is not prescribed by the POPI Act. Unlawfully obtaining personal information requires an intentional unlawful act and will always be a risk to the protection of private information when a person wilfully decides to act unlawfully.

Enforcement Notices Per Contravening Action And Industry

Objective Of The Analysis

A summary was made of all the enforcement notices issued to identify if there were any prevalent contravening actions or industries that were affected by it. The summaries can be obtained in Tables 10 and 11.

Findings And Deductions

Only 11 enforcement notices were issued between April 2010 and December 2013 and 73% of them were issued in terms of sensitive personal information breaches. The number of enforcement notices is significantly lower than the number of undertakings (130) and monetary penalties (51) issued by the ICO.

Table 10: Enforcement Notices By Contravening Action

Contravening Action	Number	Sensitive	Not Sensitive
Unencrypted laptop/s stolen.	4	4	0
Excessive data gathering by CCTV cameras and processing thereof.	2	1	1
Hard copy of private information was provided to wrong recipient/s.	1	1	0
Private information e-mailed to wrong recipient/s.	1	1	0
Illegally obtaining personal information without data subject's approval.	1	1	0
Failure to provide information from data subject request within 40 days.	1	0	1
Direct marketing: Making unsolicited phone calls.	1	0	1
TOTAL	11	8	3

The only contravening actions that occurred more than once were the theft of unencrypted laptops and the excessive data gathering with CCTV cameras. The ICO instructed three police stations and one council office to ensure that all electronic storage devices are encrypted before it is used. The ICO also instructed another police station and a council office to stop collecting excessive data with CCTV cameras with immediate effect and to responsibly destroy all data collected by it.

Table 11: Enforcement Notices By Industry

Industry	Number	Sensitive	Not Sensitive
Police	4	3	1
Social Services	2	2	0
Unspecified / Various Council Services	2	1	1
Transport	1	1	0
Technology - Knowledge management	1	1	0
Energy Service	1	0	1
TOTAL	11	8	3

Four police stations had notices imposed on them of which three were instructed to implement the compulsory use of encryption software on secondary storage devices (ICO, 2013b) and one was instructed to stop the excessive data gathering via CCTV cameras (ICO, 2013g). The enforcement notices for the social services was for the vigorous and compulsory training in data protection after sensitive personal data were exposed by providing a record containing private information to a wrong recipient (ICO, 2011k); the other instance included the sending of an e-mail to an incorrect recipient (ICO, 2012p). The council services received enforcement notices to instruct that data requested, in terms of a data subject request, is to be disclosed within 40 days after the request was received (ICO, 2012o) and that the unencrypted storage devices are to be encrypted in the future. An international technology company - Google Inc. - was also served with an enforcement notice to ensure that they destroy all data collected via their street view vehicles (ICO, 2013f).

CONCLUSION AND AREAS FOR FUTURE RESEARCH

If the South African Information Regulator performs its duties in line with the ICO, as expected by De Stadler (2013) and Tubbs (2014), it can be anticipated that the Information Regulator might initially prefer to make use of a lighter form of correctional actions in an attempt to motivate and educate organisations to become compliant with the POPI Act. The ICO selected to start their enforcement regime by using undertakings as a precursor to the more harsh action of huge monetary penalties to encourage organisations to become compliant with the DPA (ICO, 2011g), and they have gradually started to shift their focus to more severe punishment.

From the previously discussed findings, it can be deduced that any industry that manages special or sensitive personal information, like the health and social services industries, are exposed to a greater risk of data protection breaches and will be required to implement more stringent protection processes in their standard operating procedures concerning data protection than industries that do not manage sensitive personal information (DPA, 1998; POPI, 2013). This is supported by the findings in Tables 4 and 7 which indicated the high incident rates in terms of data breaches in the health and social services industries. The enforcement of the POPI Act will be on a complaint-driven system, similar to that in the UK, and it can also be argued that data subjects will be more prone to complain about a breach in personal data that they deem sensitive in nature than personal data that is not.

It was expected that all data breaches by UK businesses would be electronic in nature, but a number of the breaches constituted the compromise of physical paper copies of documents that contained personal information. Documents were misplaced or lost within an organisation and removed from the businesses for legitimate reasons, e.g. to perform work at home, but the documents were stolen or lost before they were returned to the office the following day. Physical documents were also lost during office moves and archival storage periods. If the Information Regulator follows in the ICO's footprints, it can be expected that they will provide guidance documents to South African businesses to assist them in addressing possible risk areas like these. It can be argued that where human intervention is required in a process, the risk of a data protection breach cannot be completely removed due to the inherent fallibility that exists within all humans (Reason, 2000, p.2). These inherent risks should, however, be addressed by the implementation of various appropriate steps and procedures to reduce the risk of human error to an acceptable or reasonable level.

The loss of unencrypted computers, USB's, hard drives, cd's, dvd's, back-up tapes, etc. could have been completely avoided if the secondary electronic storage devices used were encrypted with approved encryption software. It was found that many data controllers and data subjects were under the impression that if a storage device requested a password from the user, it was in fact already encrypted or sufficiently protecting the personal data stored on it, but that was not the case. Specialised encryption software is something additional to the implementation of passwords on their own and the ICO provides guidance on encryption criteria to be followed by data controllers (ICO, 2012l) and could also be consulted by South African companies if they require assistance in this regard.

The monetary fines imposed for unsolicited marketing techniques were significant and completely avoidable. South African direct marketing companies will have to ensure that they act in terms of the requirements of the POPI Act to avoid similar fines.

Wilful criminal acts by individuals to steal, obtain, disclose, or compromise personal data - for any reasons - should be earnestly considered by companies that manage personal information. Personal data have become a commodity with monetary value, and money could be earned by selling the data to the highest bidder. People can misuse their position at a company or institution to illegally obtain information on someone that they would not have been able to do otherwise. Data can also be stolen from a previous workplace to enable a person to set up shop elsewhere and to use the previous employer's contacts to canvas for new business. There are many reasons that might motivate employees to wilfully breach the data protection policies of a company and will therefore not completely be avoidable. The seriousness of the offence should be highlighted during staff training sessions on data protection to ensure that employees understand the significance of adherence to the company policies in this regard and to serve as a warning. Staff must understand that contraventions of this nature might lead to weighty penalties for the company, disciplinary actions for the offending employees; and, in severe cases, it could also lead to imprisonment.

It is clear that all South African businesses that manage personal information, albeit sensitive or not, must get their house in order to ensure compliance with the POPI Act. This will include the creation of data protection procedures and the training of all staff that has access to and/or maintains personal information, as a number of contraventions occurred due to a general unawareness of data protection principles and could have been avoided with appropriate and timely staff training. The ICO provides a number of guidance notes that could be consulted by South African companies for direction until the South African Information Regulator provides its own guidance documents. Some of the guidance documents issued by the ICO include guidance on data protection (ICO, 2010b), a code of practice for online personal information (ICO, 2011j), and a general guidance on IT security (ICO, 2012a), as well as specific guidance notes for a few different industries, e.g. charities (ICO, n.d.-a), police and justice (ICO, n.d.-i), education (ICO, n.d.-b), finance (ICO, n.d.-d), health (ICO, n.d.-e), local authority (ICO, n.d.-f), marketing (ICO, n.d.-g), MP's and political parties (ICO, n.d.-h), as well as guidance to small businesses (ICO, n.d.-j).

From the study, it is confirmed that hefty monetary penalties and other enforcement actions will be issued by the South African Information Regulator if serious contraventions are proven. In addition, it will also be able to impose prison sentences to individuals who represent guilty responsible parties. The impact of negative publicity

generated by the Information Regulator for any confirmed contraventions, in terms of the POPI Act, on a company's reputation should also be considered as it could be detrimental to the future existence of the company.

This article addresses the uncertainty that awaits the South African business environment about what can be expected when the Information Regulator is appointed by the government and the POPI Act is enforced. Several of the contraventions that occurred in the UK could have been avoided if the appropriate and necessary safeguarding procedures were implemented in the businesses. The ICO provides several resources that South African companies can use to assist them in getting their house in order on time. This article also found that this legislation will not only impact information stored electronically, but also information that which is stored on physical paper copies of documents. This article sheds some light on what could be expected in the unknown future for South Africa in terms of the enforcement of the POPI Act.

The Information Regulator can also use the information in the summaries from this study to form an understanding of how the ICO generally dealt with specific contravening actions and it could assist them in deciding how they should act in similar circumstances. This article refers to various guidance documents created by the ICO to assist the UK businesses in the implementation of processes to safeguard themselves against data protection violations. The Information Regulator can also use this article as guidance when deciding which documents they should create with urgency as part of their education and training responsibility to South African businesses and the public.

A possible area for further research includes a comparison of the actual enforcement actions taken by the Information Regulator in the future to the findings in this article and to explore any significant differences. Another area would be to identify specific data protection risks linked to different industries and to provide specific procedures to address the risks identified. An example of this could include the exploration of data protection practices used and risks linked to academic researchers who use or process personal information as part of their research actions. The underlying data of the summaries set out in this article, with the accompanying uniform resource locators to the different enforcement notices, can also be published so that it can be used by other researches if required.

AUTHOR INFORMATION

Michelle de Bruyn is a qualified Chartered Accountant of South Africa and is currently employed by the School of Accountancy at the University of Stellenbosch where she is a lecturer in Information Systems for undergraduate accounting students. She has obtained a B. Accountancy and B. Accountancy (Honours) degree at the University of Stellenbosch. Email: debruynm@sun.ac.za.

REFERENCES

1. Basson, B. (2014). *The right to privacy: how the proposed POPI Bill will impact data security in a Cloud Computing environment* (Masters Dissertation, Stellenbosch: Stellenbosch University).
2. Berry, C. (2014). Risk management: IT: protect your business' most valuable asset. *Accountancy SA, 2014* (February), 40-41.
3. Cetinkaya, V. (2013). Protecting Personal Data. *LMN IT Board security Seminar*. Retrieved 9 April, 2014 from http://ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/ico-presentation-protecting-personal-data-20131113.pdf.
4. Clarke, R. (1989). The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law. *Australian National University Unpublished Working Paper Retrieved 22 October, 2013* http://www.rogerclarke.com/DV/PaperOECD.html.
5. Constitution of the Republic of South Africa No 108 of 1996 (RSA).
6. Data Protection Act 1998 (UK).
7. De Stadler, E. (2013). Intro to POPI (part 5): Rethinking privacy policies. *Juta's Consumer Law Review, May/June*. Retrieved 21 May 2014 from http://www.esselaar.co.za/legal-articles/intro-popi-part-5-rethinking-privacy-policies.
8. DPA *vide* Data Protection Act. (1998).

9. Fox, S., Gorrill, M., Webb, L., & Parker, R. (2010). *Communicating enforcement activities* (pp. 1–11). Retrieved 28 October 2013 from http://www.ico.org.uk/enforcement/~/media/documents/library/Corporate/Detailed_specialist_guides/ico_enforcement_communications_policy.ashx.Freedom of Information Act 2000 (UK).
10. Greenleaf, G. (2013a). Chapter 10: Data protection in a globalised network. In Brown, I. [ed]. *Research handbook on governance of the Internet.* Northampton, MA: Edward Elgar. p221- 259.
11. Greenleaf, G. (2013b). Global Data Privacy Laws 2013: 99 Countries and Counting. *Privacy Laws & Business International Report*, (123), 10-13.
12. Greenleaf, G. (2013c). Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. *Journal of Law, Information & Science (September, 2013-40)*. Retrieved 9 June, 2014 from http://ssrn.com/abstract=2280877.
13. Heyink, M. (2011). *Protection of Personal Information Guidelines for Law Firms*. Law Society of South Africa. South Africa. Retrieved 14 April, 2014 from http://www.lssa.org.za/upload/Protection of Personal Information Guideline 2011 v1_0 110517(1).pdf.
14. ICO *vide* Information Commissioners Office.
15. Information Commissioners Office. (2008). *CCTV code of practice*. UK. Retrieved 28 May, 2014 from http://ico.org.uk/for_the_public/topic_specific_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx.
16. Information Commissioners Office. (2010a). *Google Inc - Undertaking*. UK. Retrieved 3 April, 2014 from http://breachwatch.com/wp-content/uploads/2012/10/2010-11-Google-Undertaking.pdf.
17. Information Commissioners Office. (2010b). *The Guide to Data Protection*. UK. Retrieved 14 April, 2014 from http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf.
18. Information Commissioners Office. (2011a). *Council sent benefit details to wrong recipients - News Release*. UK. Retrieved from http://ico.org.uk/~/media/documents/pressreleases/2011/isle_of_anglesey_undertaking_news_release_20100218.ashx.
19. Information Commissioners Office. (2011b). *Customer data thieves made to pay £73 700*. UK. Retrieved 14 April, 2014 from http://ico.org.uk/~/media/documents/pressreleases/2011/t-mobile_news_release_20110610.ashx.
20. Information Commissioners Office. (2011c). *Dartford and Gravesham NHS Trust - Undertaking*. UK. Retrieved from http://breachwatch.com/wp-content/uploads/2012/08/2011-10-Dartford-and-Gravesham-NHS-Trust-Undertaking.pdf.
21. Information Commissioners Office. (2011d). *Freehold Community School - Undertaking*, 4–5. UK. Retrieved from http://breachwatch.com/wp-content/uploads/2012/08/2011-04-Freehold-Community-School-Undertaking.pdf.
22. Information Commissioners Office. (2011e). *Gwent Police - Undertaking*. UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-02-Gwent-Police-Undertaking.pdf.
23. Information Commissioners Office. (2011f). *ICO Fines former ACS Law boss for lax IT security*. UK. Retrieved 5 April, 2014 from http://ico.org.uk/~/media/documents/pressreleases/2011/monetary_penalty_acslaw_news_release_20110510.ashx.
24. Information Commissioners Office. (2011g). *Information Commissioner's Annual Report and Financial Statements 2010/11 Information is the currency of democracy.* UK (pp. 1–86). Retrieved 29 October, 2013 from http://www.ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/annual_report_2011.ashx.
25. Information Commissioners Office. (2011h). *Kirklees Metropolitan Council - Undertaking*. UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-07-Kirklees-Metropolitan-Council-Undertaking.pdf.
26. Information Commissioners Office. (2011i). *NHS Liverpool Community Health - Undertaking.* UK. Retrieved 3 December from http://breachwatch.com/wp-content/uploads/2012/08/2011-04-NHS-Liverpool-Community-Health-Undertaking.pdf.

27. Information Commissioners Office. (2011j). *Personal information online - code of practice*. UK. Retrieved from http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx.
28. Information Commissioners Office. (2011k). *Powys County Council - Enforcement Notice*. UK. Retrieved 3 DECEMBER, 2013 from http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/Powys_cc_enforcement_notice_ENF0386991.ashx.
29. Information Commissioners Office. (2011l). *Raisa Saley - Undertaking*. UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-07-Raisa-Saley-Undertaking.pdf.
30. Information Commissioners Office. (2011m). *Sarah Phillimore - Undertaking*. UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-03-Phillimore-Undertaking.pdf.
31. Information Commissioners Office. (2011n). *Scottish Childern's Reporter Administration*. UK. Retrieved 13 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-09-Scottish-Childrens-Reporter-Administration-Undertaking.pdf.
32. Information Commissioners Office. (2011o). *Somerset County Council - Undertaking.* UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-05-Somerset-County-Council-Undertaking.pdf.
33. Information Commissioners Office. (2011p). *Spectrum Housing Group - Undertaking.* UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-10-Spectrum-Housing-Group-Undertaking.pdf.
34. Information Commissioners Office. (2011q). *Surbiton Children's Centre Nursery - Undertaking.* UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-06-Surbiton-Childrens-Centre-Nursery-Undertaking.pdf.
35. Information Commissioners Office. (2012a). *A practical guide to IT security - Ideal for the small business – Guidance note*. UK. Retrieved 30 May, 2014 from http://ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/it_security_practical_guide.pdf.
36. Information Commissioners Office. (2012b). *Belfast Health & Social Care Trust – Monetary Penalty*. UK. Retrieved 5 April, 2014 from http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/bhsct_trust_monetary_penalty_notice_BHSCT.ashx.
37. Information Commissioners Office. (2012c). *Brighton and Sussex University Hospitals NHS Foundation Trust - Monetary Penalty Notice*. UK. Retrieved 12 December, 2013 from http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/bsuh_monetary_penalty_notice.ashx.
38. Information Commissioners Office. (2012d). *City of York Council - Undertaking*. UK. Retrieved 3 December, 2013 from http://breachwatch.com/wp-content/uploads/2012/08/2011-04-City-of-York-Council-Undertaking.pdf.
39. Information Commissioners Office. (2012e). *Draft Anonymisation code of practice*. UK. Retrieved 6 June, 2014 from https://www.ico.org.uk/Global/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx.
40. Information Commissioners Office. (2012f). *Guidance on the rules on use of cookies and similar technologies*. UK. Retrieved 28 May, 2014 from http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx.
41. Information Commissioners Office. (2012g). *Holroyd Howe Independent Ltd - Undertaking*. UK. Retrieved 3 December, 2013 from http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/hhi_ltd_undertaking.ashx.
42. Information Commissioners Office. (2012h). *ICO Annual Report and Financial Statements 2011/12 In the Rights space at the right time*. UK. Retrieved 29 October, 2013 from http://www.ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/

annual_report_2012.ashx.
43. Information Commissioners Office. (2012i). *Identity and Passport Service - Undertaking*. UK. Retrieved 3 December, 2014 from http://breachwatch.com/wp-content/uploads/2012/08/2011-02-Identity-and-Passport-Service-Undertaking.pdf.
44. Information Commissioners Office. (2012j). *IT asset disposal for organisations – guidance document.* UK. Retrieved 6 June, 2014 from http://ico.org.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Detailed_specialist_guides/it_asset_disposal_for_organisations_20121_pdf.ashx.
45. Information Commissioners Office. (2012k). *Midlothian Council - Monetary Penalty Notice*. UK. Retrieved 5 April, 2014 from http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/midlothian_council_monetary_penalty_notice.ashx.
46. Information Commissioners Office. (2012l). *Our approach to encryption – guidance document*. UK. Retrieved 28 May, 2014 from http://ico.org.uk/news/current_topics/Our_approach_to_encryption.
47. Information Commissioners Office. (2012m). *Scottish Borders Council - Monetary Penalty Notice*. UK. Retrieved 5 April, 2014 from http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Notices/scottish_borders_council_monetary_penalty_notice.ashx.
48. Information Commissioners Office. (2012n). *South Yorkshire Police - Undertaking*. UK. Retrieved 3 December, 2013 from http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/south_yorkshire_police_undertaking.ashx.
49. Information Commissioners Office. (2012o). *Staffordshire County Council – Enforcement Notice*. UK. Retrieved 3 December, 2013 from http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/staff_cc_enforcement_notice.ashx.
50. Information Commissioners Office. (2012p). *Stoke-on-Trent City Council - Enforcement Notice*. UK. Retrieved 3 December, 2013 from http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/stoke_city_council_enforcement_notice.ashx.
51. Information Commissioners Office. (2013a). *Barclays Bank employee prosecuted for illegally accessing customer's account.* UK. Retrieved 3 April 2014 from http://ico.org.uk/news/latest_news/2013/barclays-bank-employee-prosecuted-for-illegally-accessing-customer-account-25093013.
52. Information Commissioners Office. (2013b). *Derbyshire Police - Enforcement Notice*. UK. Retrieved from http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/Derbyshire-Police-Authority-Enforcement-Notice.pdf.
53. Information Commissioners Office. (2013c). *Direct marketing guide*. UK. Retrieved 5 April, 2014 from http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf.
54. Information Commissioners Office. (2013d). *East Riding of Yorkshire Council - Undertaking*. UK. Retrieved 3 December, 2013 from http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/east_riding_undertaking.ashx.
55. Information Commissioners Office. (2013e). *Framework used to guide ICO staff in determining the appropriate amount of a monetary penalty* (pp. 0–2). UK. Retrieved 2 April, 2014 from http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_framework_to_determine_amount_penalty.ashx.
56. Information Commissioners Office. (2013f). *Google Inc - Enforcement Notice*. UK. Retrieved from http://www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/google-inc-enforcement-notice-11062013.pdf.
57. Information Commissioners Office. (2013g). *Hertfordshire Consabulary - Enforcement Notice*. UK. Retrieved 3 December, 2013 from http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf.

58. Information Commissioners Office. (2013h). *Information Commissioner's Annual Report and Financial Statements 2012/2013 Independant, authoritive, forward looking*. UK. Retrieved 29 October, 2013 from http://www.ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx.
59. Information Commissioners Office. (2013i). *Minister of Justice - Monetary Penalty Notice*. UK. Retrieved 5 April, 2014 from http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/moj-monetary-penalty-notice-20131015.pdf.
60. Information Commissioners Office. (2013j). *NHS Surrey c/o Department of Health Regional Legacy Management Team - Monetary Penalty Notice*. UK. Retrieved 12 December, 2013 from http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/nhs-surrey-monetary-penalty-notice.pdf.
61. Information Commissioners Office. (2013k). *Sony Computer Entertainment Europe Limited- Monetary Penalty Notice*. UK. Retrieved 3 Arpil, 2014 from http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Notices/google-inc-enforcement-notice-11062013.pdf.
62. Information Commissioners Office. (2013l). *Sony fined £ 250,000 after millions of UK gamers' details compromised – news report*. UK. Retrieved 23 October, 2013 from http://www.ico.org.uk/news/latest_news/2013/ico-news-release-2013.
63. Information Commissioners Office. (2014a). *Campaign groups reminded of need to abide by privacy rules during Scottish referendum debate*. UK. Retrieved 9 April from http://ico.org.uk/news/latest_news/2014/campaign-groups-reminded-of-need-to-abide-by-privacy-rules-18032014.
64. Information Commissioners Office. (2014b). *Civil monetary penalties issued*. UK. Retrieved 9 April, 2014 from http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Research_and_reports/civil-monetary-penalties.csv.
65. Information Commissioners Office. (2014c). *Data breaches and regulatory activities in the UK.* UK. Retrieved 3 April, 2014 from http://breachwatch.com/.
66. Information Commissioners Office. (2014d). *Enforcement notices*. UK. Retrieved 2 April, 2014 from http://ico.org.uk/enforcement/notices.
67. Information Commissioners Office. (2014e). *Monetary penalty notices issued under the Data Protection Act 1998.* UK. Retrieved 5 April, 2014 from http://ico.org.uk/enforcement/fines.
68. Information Commissioners Office. (2014f). *Prosecutions issued under the Data Protection Act 1998*. UK. Retrieved 3 April, 2014 from http://ico.org.uk/enforcement/prosecutions.
69. Information Commissioners Office. (2014g). *Undertakings issued under the Data Protection Act 1998*. UK. Retrieved 3 April, 2014 from http://ico.org.uk/enforcement/undertakings.
70. Information Commissioners Office. (n.d.-a). *Charity Guidance*. UK. Retrieved 4 June, 2014 from http://ico.org.uk/for_organisations/sector_guides/charity.
71. Information Commissioners Office. (n.d.-b). *Education Guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/education.
72. Information Commissioners Office. (n.d.-c). *Enforcement - What actions can we take?* UK. Retrieved 4 April, 2014 from http://ico.org.uk/enforcement.
73. Information Commissioners Office. (n.d.-d). *Finance guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/finance.
74. Information Commissioners Office. (n.d.-e). *Health Guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/health.
75. Information Commissioners Office. (n.d.-f). *Local authority Guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/local_authority.
76. Information Commissioners Office. (n.d.-g). *Marketing Information rights Guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/marketing.
77. Information Commissioners Office. (n.d.-h). *MPs and political parties guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/political.
78. Information Commissioners Office. (n.d.-i). *Police, Justice and Borders guidance*. UK. Retrieved 4 June

from http://ico.org.uk/for_organisations/sector_guides/police_justice.
79. Information Commissioners Office. (n.d.-j). *Small Business Guidance*. UK. Retrieved 4 June from http://ico.org.uk/for_organisations/sector_guides/business.
80. IQ Business (2014). Are South African Companies Prepared for POPI? *Accountancy SA*, (February), 34–37.
81. Justice Committee. (2012). The functions, powers and resources of the Information Commissioner, *Ninth Report of Session 2012 – 13*. Retrieved 27 May, 2014 from http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/962/962.pdf.
82. Magee, K. (2011). Reputation Survey : Sony's reputation damaged by breach harmed the firm's reputation and made them more cautious, *PR Week* (May). Retrieved 9 June, 2014 from http://www.prweek.com/article/1069435/reputation-survey-sony---sonys-reputation-damaged-breach.
83. PECR *vide* Privacy Electronic Communications Regulations. (2003).
84. POPI *vide* Protection of Personal Information Act. (2013).
85. Privacy and Electronic Communications Regulations (2003). (UK).
86. Promotion of Access to Information Act No 2 of 2000 (RSA).
87. Protection of Personal Information Act No 4 of 2013 (RSA).
88. Reason, J. (2000). Human Error : Models and Management. *British Medical Journal*, *320*(7237), 768–770.
89. Schwartz, P. M. & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYU Law Review*, *86*, 1814.
90. Tubbs, B. B. (2014). How companies can gear up for POPI. *IT Web Financial*. Retrieved 15 April, 2010 from http://www.itweb.co.za/?id=71803:How-companies-can-gear-up-for-POPI.

NOTES