A Model to Assess Organisational Information Privacy Maturity against the Protection of Personal Information Act

A dissertation presented to the
Department of Information Systems

University of Cape Town

By

Charles Hinde

(HNDCHA003)

In partial fulfilment of the requirements of the degree Master of Commerce (Information Systems)

15 August 2014

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this dissertation, *A Model to Assess Organisational Information Privacy Maturity against the Protection of Personal Information Act,* from the work(s) of other people has been attributed, and has been cited and referenced.

3. This proposal, *A Model to Assess Organisational Information Privacy Maturity against the Protection of Personal Information Act* is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

5. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is our own work.

6. I have not falsified or manufactured any data, and declare that all data was ethically collected.

Signature: Signed by candidate

Date: 15 August 2014

Full Name of Student: Charles Hinde

Student Number: HNDCHA003

Preface

I would like to thank the following people, without whom this dissertation would never have been written:

- My partner, Helen Macdonald, who provided me with the time, space and opportunity to write this thesis and whose support has been invaluable. Your indomitable strength is an inspiration.

- My family, in particular my daughters, for putting up with my absence, but keeping me involved. It's time for me to give back!

- Katherine Thompson for her invaluable input and generous heart.

- Aubrey Davies for the continued support throughout this re-education process

- Dr Jacques Ophoff for his mentorship, guidance and advice.

TABLE OF CONTENTS

List of Tables

List of Figures

Abstract

Reports on information security breaches have risen dramatically over the past five years with 2014 accounting for some high-profile breaches including Goldman Sachs, Boeing, AT&T, Ebay, AOL, American Express and Apple to name a few. One report estimates that 868,045,823 records have been breached from 4,347 data breaches made public since 2005 (Privacy Rights Clearing House, 2013). The theft of laptops, loss of unencrypted USB drives, hackers infiltrating servers, and staff deliberately accessing client's personal information are all regularly reported (Park, 2014; Privacy Rights Clearing House, 2013).

With the rise of data breaches in the Information Age, the South African government enacted the long awaited Protection of Personal Information (PoPI) Bill at the end of 2013. While South Africa has lagged behind other countries in adopting privacy legislation (the European Union issued their Data Protection Directive in 1995), South African legislators have had the opportunity to draft a privacy Act that draws on the most effective elements from other legislation around the world.

Although PoPI has been enacted, a commencement date has still to be decided upon by the Presidency. On PoPI's commencement date organisations will have an additional year to comply with its requirements, before which they should: review the eight conditions for the lawful processing of personal information set out in Chapter three of the Act; understand the type of personal information they process; review staff training on mobile technologies and limit access to personal information; ensure laptops and other mobile devices have passwords and are preferably encrypted; look at the physical security of the premises where personal data is stored or processed; and, assess any service providers who process information on their behalf.

With the demands PoPI places on organisations this research aims to develop a prescriptive model providing organisations with the ability to measure their information privacy maturity based on "generally accepted information security practices and procedures" (Protection of Personal Information Act, No.4 of 2013, sec. 19(3)).

Using a design science research methodology, the development process provides three distinct design cycles: 1) conceptual foundation 2) legal evaluation and 3)

organisational evaluation. The end result is the development of a privacy maturity model that allows organisations to measure their current information privacy maturity against the PoPI Act.

This research contributes to the knowledge of how PoPI impacts on South African organisations, and in turn, how organisations are able to evaluate their current information privacy maturity in respect of the PoPI Act. The examination and use of global best practices and standards as the foundation for the model, and the integration with the PoPI Act, provides for the development of a unique yet standards-based privacy model aiming to provide practical benefit to South African organisations.

1. INTRODUCTION

Achieving privacy is one of the most challenging exercises when dealing with any kind of information, particularly personal information. While the IT industry has been in a technological arms race with hackers and fraudsters to limit their access to personal information, it would seem that policy and behaviour need to be addressed simultaneously. During an interview for this dissertation, the editor of the Security and Privacy magazine echoed these sentiments, “a lot of technologists thought that technology would solve privacy problems; now I think they are realizing that it takes a combination of technology and policy -- so the conversation is more informed by behavioral scientists than it used to be.” (S.Phleeger, personal communication, November 13, 2013)

On 26 November 2013 the president signed the Protection of Personal Information Act (PoPI) into law, and almost all businesses across all industries in South Africa will be required to comply with stringent requirements regarding why and how they collect, use, disclose and store personal information belonging to both natural and juristic persons.

While the South African government has lagged behind other countries in adopting privacy legislation, South African legislators have had the opportunity to draft a privacy Act that draws on the most effective elements from other legislation around the world. The rapid and continued growth in technology and the global response to the commercialisation of personal information are seen as drivers for developing legislation that will encompass the privacy of South African citizens (Matthes, 2014).

While independent reports indicate a daunting task ahead for PoPI compliance for South African organisations, it also reveals an opportunity to utilise global best practice standards and frameworks to initiate the creation of an information privacy management program (Price Waterhouse Coopers, 2011). Utilising global best practice frameworks and standards for privacy and technical controls can provide an organisation (from small to medium enterprises (SME) to multi-national corporations) with a valuable starting point when addressing an information privacy management program (Pearson, 2012).

1.1 Problem Statement

Current popular media indicates that South African organisations are not ready for the implementation of the PoPI Act (Grant Thornton, 2014; Lamprecht, 2013). The penalties for non-compliance are severe with organisations facing fines of up to R10 million or the designated privacy officer (or CEO/owner) the prospect of 10 years in prison (Protection of Personal Information Act, No.4 of 2013, section 107(a)). In addition, civil class action is available as punitive damages, which could lead to significant monetary loss, and possible reputational damage to organisations.

While PoPI is not a technical piece of legislation, it does add an extra layer of administration. Michiel Jonker, Director: IT Advisory at Grant Thornton, says the costs of implementing PoPI will place significant cost pressures on big business due to the employment of additional specialised personnel, including expensive and highly-skilled privacy officers, the contracting of IT and business auditing service providers; and the need for specialist legal consultants to review existing agreements which may exist with third party companies (Grant Thornton, 2014). Large organisations will not be the only sector impacted as approximately 91% of the formal business entities in South Africa are SMEs with a turnover of less than R10 million (Abor & Quartey, 2010; Cornish, 2013), meaning the cost of utilising specialist consultants in the pursuit of PoPI-compliance becomes more difficult.

Outside of hiring specialist consultants there are opportunities for organisations to begin the PoPI-compliance process:

- review the eight conditions for the lawful processing of personal information set out in Chapter three of the Act;
- understand the type of personal information being processed within the organisation, and how it complies with the eight conditions outlined in chapter three of the Act;
- review staff training on mobile technologies and limit access to personal information on mobile devices and the organisation network;
- ensure laptops and other mobile devices have passwords and are preferably encrypted;
- review (or implement) policies around password use and data protection

- survey the physical security of the premises where personal data is stored or processed (CCTV, alarms, access control etc.);
- assess any service providers who process information on the organisations behalf, and seek assurances that they will also comply with PoPI.

Considering the challenges organisations face to safeguard sensitive information, **there exists the need for a tool to help South African organisations measure their information privacy maturity in relation to the newly enacted PoPI Act of 2013.**

1.2 Research Objective

The primary objective of this research is the development of a prescriptive model for South African organisations to measure their information privacy maturity in relation to the newly enacted PoPI Act of 2013, which is both easy to use and useful. To achieve this, a number of secondary objectives need to be addressed:

- investigate current best practice frameworks within privacy, information security, personal data protection, data quality, electronic archiving, and risk management;
- determine the level of compliance required for organisations based on PoPI requirements;
- understand the factors that would encourage the use of an artefact within an organisation.

The secondary objectives form a whole which, when integrated, should contribute towards the successful development of the intended artefact (model). However, the mere design of an artefact may not encourage its utilisation – particularly if there is ambivalence towards compliance with legislation (SMEs for instance). Creating a tool that has perceived usefulness and perceived ease of use is as important as providing a functional tool – there is no benefit in developing an artefact that provides measurable value, yet is not utilised due its complexity or unfriendly user interface (Davis, Bagozzi, & Warshaw, 1989). The final instantiation of the model aims to provide an easy to use tool for organisational use in pursuit of measuring privacy maturity.

1.3 Scope of Study

This research intends to review a range of privacy-related legislation and current global best practice frameworks and standards. While South Africa has recently enacted the PoPI Act, it is based on legislation from Europe (EU Directive 95/46/EC) and the United Kingdom (Data Protection Act) (Cornish, 2013). Reviewing these two Acts will provide context for PoPI. Numerous institutions develop best practice standards which have global acceptance, the National Institute of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA) and the International Organization for Standardization (ISO) for example. Researching global best practices will be limited to privacy and information security with the intention of integrating PoPI and providing a local integration with the global standard.

1.4 Assumptions and Limitations

While the objective of this research is to develop a prescriptive model that provides organisations with the ability to measure their privacy maturity, it is assumed that input will be required from both a legal and organisational perspective to allow for a more holistic artefact. Limitations in the scope of the model may be present due to the time and size constraints imposed by the Master's dissertation deliverable.

1.5 Ethical Considerations

All personal or identifiable information of research participants, or the organisations they work for, has been anonymised. This research was approved by the UCT Research Ethics Committee.

1.6 Outline of the Study

Having outlined the problem statement and scope of this dissertation, Chapter 2 provides a literature review of personally identifiable information, and the context of PoPI within privacy legislation. Chapter 3 outlines the research design and methodology of this study, followed by the design, instantiation and evaluation of the artefact developed (Chapters 4-7). Finally, Chapter 8 summarises and concludes the dissertation.

2. LITERATURE REVIEW

This literature review places PoPI in context in respect of privacy, the growth in technology driving new legislation, and the global response to the commercialisation of personal information. The literature review builds a picture of the influences involved in drafting PoPI, the main drivers around securing the processing and flow of personal information, and the impact it will have on organisations within South Africa.

2.1 What is Privacy – An Overview

The Oxford Dictionary (2014) defines *privacy*, as "a state in which one is not observed or disturbed by other people". A person's right to privacy is extended further than being merely "left alone" and includes the right to having control over his or her personal information and the ability to conduct their personal affairs relatively free from unwanted intrusions (Neethling, Potgieter, & Visser, 1996). Considered a fundamental human right it is recognised by the Universal Declaration of Human Rights[1], the International Covenant on Civil and Political Rights[2], and in many other international and regional treaties (Banisar & Davies, 1999). Although privacy has deep seated roots in history (the law of privacy can be traced as far back as 1361, when the English Justices of the Peace Act provided for the arrest of peeping toms and eaves droppers (Banisar & Davies, 1999)), it is considered one of the most difficult human rights to define.

In 1960 William Prosser determined four types of harmful activities classed as privacy infringements (Solove, 2006):

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.

2. Public disclosure of embarrassing private facts about the plaintiff.

3. Publicity which places the plaintiff in a false light in the public eye.

4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

[1] Universal Declaration of Human Rights, adopted and proclaimed by the United Nations General Assembly resolution 217 A (III) of December 10, 1948.
[2] International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly on 16 December 1966

Over the past 50 years these infringements have become almost antiquated with the breathtaking rise of the information age. An array of different privacy problems have emerged due to the growth in new technologies since Prosser devised his four categories – many of them not fitting into any of the four.

While the definition of privacy describes how far society can intrude into a person's affairs, privacy advocates describe privacy as having several aspects or categories (Banisar & Davies, 1999; Kim, 2006; Marsoof, 2008):

- *information privacy*, involving the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
- *bodily privacy*, concerning the protection of people's physical beings against invasive procedures such as drug testing and cavity searches;
- *privacy of communications*, covering the security and privacy of mail, telephones, email and other forms of communication; and
- *territorial/physical privacy*, concerning the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

To assist lawmakers with the complexity and difficulty in addressing privacy in the current Information Age, Solove (2006) has put forward a taxonomy to "identify and understand the different kinds of socially recognized privacy violations" (p. 480):

Table 1: Taxonomy of privacy violations (Solove, 2006)

Information Collection (the process of data gathering)	
Surveillance	Both public and private, includes audio and video.
Interrogation	Pressuring individuals to divulge information.
Information Processing (the use, storage, and manipulation of data that has been collected)	
Aggregation	The gathering together of information about a person.
Identification	The association of data with a particular human being.
Insecurity	Caused by the way information is handled and protected
Secondary Use	The use of data for purposes unrelated to the purposes for which it was initially collected without the data subject's consent.
Exclusion	Denied from participating in the use of one's personal data; by not being informed about how that data is used; not being able to do anything to affect how it is used.
Information Dissemination (the revelation of personal data or the threat of spreading information)	
Breach of Confidentiality	The revelation of true information about a person due to the violation of trust in a specific relationship
Disclosure	The revelation of true information about a person to others (no violation of trust).
Exposure	The exposing to others of certain physical and emotional attributes about a person.
Increased Accessibility	Information that is already available to the public is made easier to access (increases the possibility of disclosure).
Blackmail	Involves a threat of disclosure of information rather than an actual disclosure of it.
Appropriation	The use of one's identity or personality for the purposes and goals of another.
Distortion	The manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public - the information revealed is false and misleading.
Invasion (harm not caused by information)	
Intrusion	Unwanted social invasions, which includes non-spatial incursions such as spam, junk mail, junk faxes, and telemarketing.
Decisional Interference	Involves governmental interference with people's decisions regarding certain matters of their lives

While the lack of a single definition of privacy may indicate the concept is in disarray, and has been said to suffer from an “embarrassment of meanings” (Scheppele, 1988, p. 184), Costa Rican politician Fernando Volio Jiménez is quoted as saying, “in one sense, all human rights are aspects of the right to privacy” (Volio, 1981, p. 184).

2.2 “Privacy” and “Data Protection”

As the technological environment has expanded since the 1960’s and the use of electronic commerce has become more ubiquitous, so the concern around privacy and personal information protection has increased (Cowles, 2001; Hurley & Mayer-Schönberger, 2000; White House, 1997; Zysman & Weber, 2001). The advent of electronic communication has removed the obstacles of distance and time when transferring information and with this has come the possibility of information or *data* being intercepted and falling into the hands of unintended parties (Marsoof, 2008).

As the digitisation of information continues into the foreseeable future the question of whether privacy is distinct from data protection needs to be answered. The Information Technology Act of India, 2000, section 2(o), provides a comprehensive definition of data:

> *...data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*

Using this definition, data protection indicates the protection of information that can be generated using computer systems. Utilising the definition of data and applying it to the categories (aspects) of *information privacy* and *privacy of communications* mentioned earlier, it becomes apparent that data protection is also an aspect of privacy.

2.3 Why is Information Privacy Important?

As the sophistication of information technology escalates, and the interconnectivity of networks providing unprecedented methods of collecting, analysing and disseminating information on individuals increases, so the concern of the invasion of privacy, or the potential of invasion, increases correspondingly (Banisar & Davies, 1999). Banisar and Davies (1999) extend the technological aspects of privacy invasion to include three important trends:

- *globalisation* removes geographical limitations to the flow of data - the development of the Internet is perhaps the best known example of a global technology;
- *convergence* is leading to the elimination of technological barriers between systems. Modern information systems are increasingly inter-operable with other systems, and can mutually exchange and process different forms of data;
- *multi-media* fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms.

Clarke (1997) provides four reasons why privacy is important, and these become more evident when considering the ease of proliferation of information, and the corresponding invasion thereof:

- Privacy is *psychologically* important: “People need private space. . . . We need to be able to glance around, judge whether the people in the vicinity are a threat, and then perform actions that are potentially embarrassing.”
- Privacy is *sociologically* important: “People need to be free to behave and to associate with others, subject to broad social mores, but without the continual threat of being observed.”
- Privacy is *economically* important: “People need to be free to innovate. International competition is fierce, so countries with high labour-costs need to be clever if they want to sustain their standard-of-living. And cleverness has to be continually reinvented.”

- Privacy is *politically* important: “People need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and threatens democracy.”

Privacy allows people to develop their individuality apart from the groups to which they belong and offers them the ability to decide what face they want others to see (Fromholz, 2000).

2.4 The Costs of Protecting Privacy

While the protection of privacy outlined by Clark (1997) offers benefits to both society and individuals it must be tempered with the associated costs. While privacy allows individuals the opportunity to decide “what face they want others to see, it is not an absolute good because it imposes real costs on society” (Fromholz, 2000, p. 465). A broadly defined privacy right allows for the opportunity of withholding true information from society therefore protecting some individual rights at the expense of others. Promoting the possibility of misinformation can have both social and economic impacts as people are less able to make fully informed decisions such as whether a “child's babysitter had been convicted for child abuse or whether a physician had a history of malpractice” (Fromholz, 2000, p. 465).

The midpoint between too little or too much privacy is what progressive governments need to find. When looking at global privacy legislation there tends to be a minimum level of privacy protection without a maximum set (Fromholz, 2000), and in the case of South African legislation “the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests” (Protection of Personal Information Act, No.4 of 2013, 2013).

2.5 Privacy Legislation

2.5.1 International Privacy Legislation

Ouside of the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966), internationally privacy has been recognised as an important right to be protected. The advent of globalisation and economic imperatives has brought with it the need for nations to cooperate at numerous levels, one of which is ensuring the privacy of individuals.

The genesis of modern privacy legislation can be traced back to the Land of Hesse in Germany in 1970 which then prompted countries like Sweden (1973), Germany (1977) and France (1977) to follow suit (Banisar & Davies, 1999). Using this early legislation as a foundation two crucial international instruments evolved – The Council of Europe's (COE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[3], and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[4]. Both instruments lay out specific rules covering the handling of electronic data which now forms the core of many global data protection laws (Banisar & Davies, 1999).

The European Union has extended the COE's 1981 legislation to take into consideration the globalisation of the information economy (Information Security Group of Africa, 2011) and currently utilises the 1995 Data Protection Directive (in January 2012 the European Commission unveiled a draft European General Data Protection Legislation which will supersede the Data Protection Directive (von Baum, 2012)).

While Europe has legislated data privacy at a national level the United States has followed an industry-based self-regulation process. This *laissez-faire* governance system, where markets set the industry agenda, has resulted in existing legislation that is reactive and issue-specific (Kobrin, 2004), and is characterised as a "patchwork quilt" (Holvast, Madsen, & Roth, 1999, p. USA–1) with no single overarching privacy law (Movius & Krup, 2009).

Globally there are many countries that now protect privacy under human rights legislation within their constitutions: Kingdom of the Netherlands (Constitution of the Kingdom of the Netherlands, 1989), Republic of the Philippines (Part III, Constitution of the Republic of the Philippines, 1987), and the Russian Federation (art 23, Constitution of the Russian Federation, 1993)[5]. While the definition of data protection may vary across international laws and declarations, Banisar and Davies (1999)

[3] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[4] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[5] For additional privacy laws by country see:
http://www.informationshield.com/intprivacylaws.html
http://www.mofo.com/privacylibrary

observe that the attributes of personal information are consistently described as being:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These attributes form part of the core of South Africa's Protection of Personal Information Act.

2.5.2 South African Privacy Legislation

In South Africa the right to privacy is protected in terms of both common law[6] and the in the Constitution of the Republic of South Africa, 1996 (section 14[7]). However, the right to privacy is not absolute and consideration is given to competing interests such as maintaining law and order, protecting commercial interests, and the administration of national social programs (South Africa Law Reform Commission, 2005). While the right to privacy is balanced with other rights entrenched in the Constitution, the recognition it has within the Constitution as a fundamental human right indicates its importance.

Outside of the Constitution (and common law) there is currently no legislation which deals specifically and fully with information protection (South Africa Law Reform Commission, 2005). In November 2000 the South African Minister of Justice and Constitutional Development requested the South African Law Reform Commission (SALRC) to investigate concerns around the protection of personal information (South Africa Law Reform Commission, 2005). In September 2003 the SALRC

[6] In terms of the common law every person has personality rights such as the right to privacy, dignity, good name and bodily integrity

[7] Section 14 of the Constitution reads as follows:

> Everyone has the right to privacy, which includes the right not to have
> a) their person or home searched;
> b) their property searched;
> c) their possessions seized; or
> d) the privacy of their communications infringed.

published a comprehensive Issue Paper for information and comment entitled "Privacy and Data Protection" (known as Project 124) and received written comment from 34 persons and institutions. In October 2005 the SALRC published a Discussion Paper with draft legislation and invited comment towards the creation of the Protection of Personal Information Bill (B9-2009).

While current legislation in the form of the Promotion of Access to Information Act (Act 2 of 2002), Electronic Communications and Transactions Act (Act 25 of 2002) and the National Credit Act (Act 34 of 2005) deal with elements of the protection of personal information, such as a data subject's right to having access to their information, the correction of their information, and the voluntary adherence to the protection of information, these sections are regarded as interim measures until specific information privacy legislation has been finalised (South Africa Law Reform Commission, 2005). The promulgation of the information protection legislation will result in amendments to the aforementioned Acts. For a list of current legislation affecting privacy within South Africa refer to Appendix A.

2.6 The Price of Non-Compliance

The rise in information security breaches over the past five years, through either malicious intent or systems weakness, has shown how vulnerable our personal information is to abuse. The theft of laptops, loss of unencrypted USB drives, hackers infiltrating servers, staff deliberately accessing client's personal information are all regularly reported (Greenberg, 2013; Privacy Rights Clearing House, 2013). While negligence and user naivety can be attributed to many incidents, the risk of fraud through organised crime should not be under estimated.

Chapter 11 of PoPI sets out the statuary offences and the associated penalties for non-compliance to any responsible party who contravenes the conditions of the Act. Transgressions while processing personal information in an unlawful manner, or without consent, are measured using section 105, and a responsible party will be guilty of an offence if:

- the contravention is of a *serious or persistent nature* (105(a)) and likely to cause *substantial damage or distress* (105(b)); and

- the responsible party knew or ought to have known that there was a risk that the *contravention would occur* (105(a)(i)) and *failed to take reasonable steps to prevent the contravention* (105(b)); or
- the responsible party knew or ought to have known that *such contravention would likely cause substantial damage or distress* to the person (105(a)(ii)) and *failed to take reasonable steps to prevent the contravention* (105(b)).

A responsible party convicted of such an offence is liable to pay a fine or to be imprisoned for a period not exceeding 10 years, or to both a fine and such imprisonment (107(a)).

If a responsible party is alleged to have committed an offence in terms of PoPI an *administrative fine can also be imposed by the Regulator, which fine may not exceed R10 million* (109(2)(c)).

While chapter 11 of PoPI deals in specific punitive action (prison terms and monetary awards), there is still the possibility of a civil action (section 99) being brought against a responsible party where the court may award an amount as damages for compensation for patrimonial (monetary losses) and non-patrimonial (99(3)(a)) loss (non-monetary loss expressed as monetary loss such as pain and suffering) suffered by an aggrieved data subject; aggravated damages (99(3)(b)) for example humiliation or embarrassment; interest (99(3)(c)); and the costs of the lawsuit (99(3)(d)) (Information Security Group of Africa, 2011).

2.7 The Protection of Personal Information Act - No.4 of 2013 (PoPI)

In May 2009 the SALRC approved the investigation into privacy and data protection that the Minister of Justice initiated in 2000. On 13 August 2009 the South African Cabinet approved the Protection of Personal Information Bill (PoPI), and four years later passed it into law, thereby protecting individuals personal information by penalising organisations and other parties that do not adequately protect personal information (Information Security Group of Africa, 2011).

The preamble to PoPI offers an insight to the direction of the legislation (Protection of Personal Information Act, No.4 of 2013):

> *everyone has the right to privacy which includes a right to protection against the unlawful collection, retention, dissemination and use of personal information which the State must respect, protect, promote and fulfil the rights in the Bill of Rights*

At a high level PoPI aims to:

- Promote the protection of personal information processed by public and private bodies;
- Introduce information protection principles so as to establish minimum requirements for the processing of personal information;
- Provide for the establishment of an Information Protection Regulator;
- Provide for the issuing of codes of conduct;
- Provide for the rights of persons regarding unsolicited electronic communications and automated decision making; and
- Regulate the flow of personal information across the borders of the Republic (Protection of Personal Information Act, No.4 of 2013)

The objective of PoPI is to regulate the processing of personally identifiable information (PII) by public and private bodies while working within international standards - particularly European legislation.

2.7.1 Personally Identifiable Information (PII)

Personally identifiable information (PII) “is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources” (University of Miami, 2014). Breaches in PII not only impact individuals in the form of identity theft, blackmail or embarrassment, but can also impact organisations in the form of loss of public trust, legal liability and remediation costs (McCallister, Grance, & Scarfone, 2010).

Chapter 1 of PoPI defines PII as “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person”. Examples of personal information include passport and ID numbers, gender and biometric

indicators, bank account and credit card details, birth dates, home address details, personal telephone numbers (both landline and mobile devices).

While chapter 1 defines PII, chapter 25 provides for the prohibition on processing of special personal information:

> Unless specifically permitted….a responsible party may not process personal information concerning a -
>
> (a) child who is subject to parental control in terms of the law; or
>
> (b) data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour
>
> (Protection of Personal Information Act, No.4 of 2013)

2.7.2 Scope and Applicability of PoPI

Chapter 2 of PoPI provides a clear indication of its scope as it applies to the processing of personal information in any recorded format - both electronic and paper-based format. Processing within PoPI is defined as:

> any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including -
>
> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
>
> (b) dissemination by means of transmission, distribution or making available in any other form; or
>
> (c) merging, linking, as well as blocking, degradation, erasure or destruction of information;

Utilising the defined words within PoPI the scope and applicability can be contextualised by saying:

> PoPI is concerned with the *processing of personal information recorded in any format by a responsible party*.

Breaking this sentence down using the PoPI definitions provides more clarity on the scope of PoPI's impact:

Processing

The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information

of personal information

Information relating to an identifiable, living natural person/identifiable existing juristic person i.e. race, gender, sex, email address, physical address

recorded in any format

Any recorded information regardless of the form including books, maps, plans or drawings

by a responsible party

Public or private bodies, alone or in conjunction with others, determines the purpose of and means for processing personal information

2.8 Organisational Information Privacy Behaviour

The implementation of PoPI will require organisations to either implement or update existing privacy policies. Greenaway and Chan (2013) suggest there is limited theory to guide academic researchers in understanding organisational information privacy behaviour's. Due to this they recommend using a two-pronged approach:

1. *Institutional Approach (IA)*: the examination of relationships between an organisation and their environments – "survival may depend more on conforming to the norms of external groups and less on succeeding as efficient producers of goods and services." (2005, p. 176). Information privacy

behaviours are primarily responses to external pressures or "institutional" forces - most firms do not choose to differentiate themselves competitively through their information privacy programs.

2. *Resource-Based View (RBV):* grounded in the economic tradition that businesses are profit-seeking entities searching "for competitive advantage based on strategic differentiation" (2005, p. 183). Unlike IA, businesses' behaviours towards privacy are based on choices that differentiate them from others – they choose to "develop their customer information resource as an important source for achieving competitive advantage" (2005, p. 182)

Table 2: Summary of theoretical explanations for information privacy behaviours (Chan & Greenaway, 2005)

Theory / Theory Attributes	Institutional Approach		Resource-based View	
	Acquiescence strategy	**Proactive strategy**	**Customer knowledge capability**	**Customer relationship capability**
Organisational goal argued by theory base	Survival		Competitive advantage	
Information privacy role in achieving organisational goal	Source for pragmatic legitimacy	Source for social legitimacy	Support for differentiation through intellectual resource	Support for differentiation through social resource
Focus of firm information privacy activities	Internal	External	Internal	External
Information privacy as a mechanism for achieving the goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organisational information management processes	Evolution of organisational privacy management processes

Greenaway and Chan (2013) argue that a single theory cannot explain the range of corporate behaviours towards privacy. Utilising IA to explain behaviour through competitive necessity and RBV to explain the pursuit of competitive advantage, allows for more theoretically-grounded research using the institutional and resource-based paradigms

2.9 Organisational Impact of PoPI

Due to the pervasive nature of personal information, be it client, customer or employee data, PoPI has the potential to touch on all industries and impact the majority of organisations, be they multi-national or Small to Medium Enterprises (SMEs). The strict parameters that govern the processing, handling, storage and destruction of personal information (client or employee) indicate that at some level all organisations will be impacted.

Legislation governing South African organisations is well established (see Appendix B). While organisations may comply with the various Acts governing their business sectors they will need to ensure that all processes involving the collection, storage, use, display, transfer, archiving, modifying, maintaining and destruction of any information which may be used to identify a person, are PoPI-compliant to avoid contravening its requirements and becoming liable to fines, civil claims, regulatory audits and/or even imprisonment (Harty, 2013).

There are no PoPI-compliance quick-fixes and any minimum requirements for compliance will involve every phase in the information lifecycle (Deloitte, 2014). Addressing these issues will necessitate reviewing and restructuring various organisational processes to ensure proper governance in various departments, including legal and regulatory; governance, risk and compliance; information technology; human resources; vendor and third-party management; marketing; and product and service development.

2.9.1 Legal and Regulatory

Legal and regulatory departments will need to ensure that all business-wide information management requirements have been identified and the required legislative compliance regulations are communicated to the applicable departments (Information Security Group of Africa, 2011).

2.9.2 Governance, Risk and Compliance

Organisations large enough to have governance, risk and/or compliance departments could consider these as the custodians of the information privacy management program. The operational implementation of the PoPI requirements will lie here. Departments engaged with personal information will need to understand the privacy requirements of PoPI, and any business processes requiring adjustment for compliance purposes need to be identified. This could include business privacy statements and policies, contracts with third party service providers around privacy, revising minimum data collection policies and retention periods, access to personal information requests from data subjects, updating reporting processes in case of a data breach, and ensuring business practices are in-line with privacy statements and policies (Information Security Group of Africa, 2011).

Dedicated governance, risk and compliance resources may not be available to SMEs, however Peterson, Meinert, Crisswell and Crossland (2007) report that "privacy policy statements represent one of the simpler and less expensive methods of increasing consumer confidence" (p. 658). While privacy policy statements are not legally binding contracts (either on an organisation's website, or used as part of an organisation's email signature) the strength and language used in the statement can have a positive impact for smaller SMEs lacking name recognition (Peterson et al., 2007).

2.9.3 Information Technology

Section 19 of PoPI explicitly states that a responsible party "must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures" (19(1)) to facilitate the secure access, processing, storage and disposal of personal information. Technical policies, standards and procedures will need to be identified and updated to ensure alignment with the business privacy management program. Appropriate preventative[8] (e.g. systems access management) and detective[9] controls (e.g. activity logs for systems

[8]Preventative controls detect problems before they arise or attempt to predict potential problems before they occur and make adjustments (Cannon, 2011).
[9]Detective controls detect and report the occurrence of an error, omission or malicious act (Cannon, 2011).

access management) need to be implemented in technical systems handling personal information (Information Security Group of Africa, 2011).

2.9.4 Human Resources

Human resources will need to ensure that employment practices and contracts of employees who have access to personal information (for example, call centre staff, payroll and finance staff) are adjusted. Training staff to understand the importance of privacy as well as updating or implementing non-disclosure agreements will be critical in this domain (Information Security Group of Africa, 2011).

2.9.5 Vendor and Third-party Management

Section 11(f) allows a responsible party to pass personal information to a third party for processing if it is for *legitimate interests.* If the third party is in a foreign country section 72 states the "recipient of the information is subject to a law, binding corporate rules, binding agreement or a memorandum of understanding" (72(1)(a)) "that effectively upholds principles for reasonable processing" (72(1)(a)(i)) and "includes provisions, that are substantially similar" (72(1)(a)(ii)) of South Africa.

These requirements will necessitate an organisation to include privacy requirements within agreements or contracts that relate to the accessing, processing or storage by a third-party, and should apply to all applicable vendor systems accessing user information throughout the information life cycle (Information Security Group of Africa, 2011).

2.9.6 Marketing

Marketing departments have been subject to legislation curbing their activities, particularly unsolicited direct marketing, via the Electronic Communications and Transactions Act of 2002 (section 45) and more recently the 2011 Consumer Protection Act (Michalsons, 2011). Chapter 8 of PoPI contains three clauses which will place additional restrictions on marketing departments around unsolicited electronic communications (clause 69), printed or electronic subscriber directories (clause 70), and automated decision making (clause 71) (Michalson, 2009).

Marketing departments will need to ensure that the personal information they use has been specifically gathered for marketing purposes and that consent has been given by the respective data subjects (Information Security Group of Africa, 2011).

2.9.7 Product and Service Development

Product and service development departments will need to ensure that the development of products or services relying on customer's personal information includes 1) the disclosure of the nature of the information being collected, 2) the intended use of the information is disclosed to the data subject, 3) mechanisms are provided for the data subject to revoke their consent to use their information, and 4) advise the data subject on the process to query, update or remove their personal information (Information Security Group of Africa, 2011).

While the above-mentioned departments may differ from organisation to organisation, and the list is in no way exhaustive, there is a sense that PoPI will have an impact on most organisations in some way. Harty, from Harty Rushmere Attorneys sums up the problem succinctly,

> *The explosion of new electronic communication tools and the Internet, which businesses use to communicate, interact and transact with their customers, means that personal information protection/privacy is a growing challenge that needs to be urgently addressed and, consequently, business operations and procedures may need to be adapted to comply with complex and demanding laws and regulations concerning personal information.* (Harty, 2013, para 2)

2.10 Privacy Frameworks and Standards

Security frameworks and global best practice standards for the governance of digital information date back to the 1980s when the UK Government recognised their growing dependence on IT. This prompted the UK Government's Central Computer and Telecommunications Agency to develop a set of standard practices to align IT management practices – the IT Infrastructure Library (ITIL) was born. As the digital domain has grown, and enterprise has become more reliant on storing, accessing and managing digital data, the necessity to establish best practice standards and frameworks has emerged (Galup, Quan, Dattero, & Conger, 2007).

Best practice organisations such as the British Standards Institution (BSI, est. 1901), the International Organization for Standardization (ISO, est. 1947), and Information Systems Audit and Control Association, (ISACA, est. 1969) to name a few, began

developing standards, benchmarks and best practice guidelines for the IS and IT domain as the industry expanded.

The concept of a *best practice* has been defined by Camp (1989) as those practices "that will lead to the superior performance of a company" (p. xi) – therefore providing the opportunity of higher performance levels. Hiebeler, Kelly and Ketteman (2012) offer a slightly different perspective and describe best practices as "the best ways to perform a business process" (p. 7) – thereby suggesting improved operational throughput. Hughes and Smart (1994) extend the definition of best practice further as "an activity or action which is performed to a standard which is better or equal to the standard achieved by other companies in circumstances that are sufficiently similar to make meaningful comparison possible" (p. 313) – introducing the concept of a measurable comparison.

Over the years the popularity and interest shown in best practice codes has become an important tool in setting the standards for corporate governance (Aluchna, 2009b). Due to best practice codes having been developed within industry, and not as legislation via Government, they are easier to adopt and less rigorous to implement, but maintain a "comply or explain" rule that allows for self-regulation (Aluchna, 2009b). In addition to self-regulation, the ISO, for example, in conjunction with auditing firms such as Deloitte and Arthur Anderson, offer certification in best practice standards which lend additional credibility to a company's governance policies. Combined with Government legislation (e.g. Electronic Communications and Transactions Act and PoPI Act) the intention is to provide investor protection, business confidence and improved corporate performance (Aluchna, 2009a).

Table 3 below provides a list of some global best practice frameworks and standards that organisations can use when considering their information privacy management program. While no single framework or standard provides a holistic solution for PoPI compliance, utilising sections from various standards will enable organisations to build towards a compliance solution.

Table 3: Summary of privacy frameworks and standards (Information Security Group of Africa, 2011)

Framework / Standard	Description
British Standard - BS10012:2009 (Personal Information Management System)	Provides guidance on the implementation of a personal information management system (PIMS) and aids British organisations in complying with the Data Protection Act.
CWA 15499-2 - Personal Data Protection Audit Framework (EU Directive EC 95/46) - Part II	Provides checklists, questionnaires and templates for preparing for a privacy audit of the EU Directive.
GAPP - Generally Accepted Privacy Principles Framework 2006	Provides guidance to design and implement privacy practices in an organisation.
ISO/IEC 29100 – Information technology - Security techniques - Privacy framework	Provides guidance concerning information and communication technology requirements for the processing of personally identifiable information.
ISO/IEC 29101 – Information technology - Security techniques - Privacy reference architecture	Provides a high-level reference architecture for planning and building information and communication technology (ICT) systems that facilitate the proper handling of personally identifiable information (PII).
ISO27001/2	Defines an overarching security framework consisting of 133 specific controls that organisations can implement through the application of a risk management process.
Control Objectives for Information and Related Technology (COBIT)	A framework created by ISACA for information technology (IT) management and IT governance. Used as a toolset to bridge the gap between control requirements, technical issues and business risks.
Standard of Good Practice (SOGP)	A business-focused, practical and comprehensive guide to identifying and managing information security risks in organisations and their supply chains.
Information Technology Infrastructure Library (ITIL)	An IT service management framework that provides guidance on the full life cycle of defining, developing, managing, delivering and improving IT services.

2.11 Changing Attitudes

While policies, procedures, contracts, governance and technical controls make up the majority of the compliance requirements, human resources and the successful implementation will rely on owners, managers and employees understanding the privacy requirements and implementing them effectively.

Aligning an organisation's employees with its strategic goals, in this case PoPI compliance, is one of the key contributing factors to achieving those goals – what

Boswell, Bingham and Colvin (2006) term an employee's "line of sight" to the organisation's strategic objectives. The effective implementation and execution of a business strategy relies on efficient communication with all employees regardless of their position or experience within the company (Ooi & Darmawan, 2011) and this will be applicable when working towards PoPI compliance.

Gagnon, Jansen and Michael (2008) consider employees to be "strategically aligned when their behaviours correspond with their organization's strategy" (p. 426) and therefore employees offer strategic commitment to support the business's strategy. The empirical evidence gathered by Gagnon et al. (2008) suggests that "strategically committed individuals are predisposed to engage in strategic-supportive behaviour, and that development of individual commitment to strategic initiatives is likely to assist the enactment of strategic transformation" (p. 438). While this "line of sight" alignment between an organisation and its employees is based on strategies in general, the successsful implementation of an information privacy management program is no different in that its success depends on the alignment of the employees within the organisation and the privacy program (Ooi & Darmawan, 2011).

According to Greenaway and Chan (2013) an organisation's decision to protect the privacy of its customer's personal information depends on whether privacy is viewed as a risk or opportunity, or whether this is an internally or externally focused activity. Greenaway and Chan provide an alignment framework based on these decisions which are presented in Table 4 below:

Table 4: Customer information privacy framework (Greenaway & Chan, 2013)

	Internal Focus *Management emphasises internal stakeholders and processes*	**External Focus** *Management emphasises external stakeholders and processes*
Risk *Privacy action seen as potentially negative and costly to the organisation*	A Minimum privacy activities to avoid breach	B Minimum privacy activities to avoid regulatory oversight
Opportunity *Privacy action seen as potentially positive and a good investment for the organisation*	C Maximise privacy-based information collection/process improvement	D Maximise privacy-based customer relationships

The four quadrants represent an organisation's privacy approach preferences (privacy perceived as a risk or opportunity; an internal or external focus) and privacy outlook constraints (e.g. reputational concerns, customer privacy assumptions, privacy culture and privacy impact of IT investments) (Greenaway & Chan, 2013).

While there is no one right way to create a privacy program, organisations need to align the program to the best fit for them. A minimalist approach (cell A) may be an effective starting point, however organisations need to be aware of changes in privacy legislation and comply accordingly. The implementation of a privacy program will be influenced by numerous challenges – complying with regulations, preventing data breaches, advances in technology, insider threats and keeping customers happy, but the critical element is to ensure the privacy program is aligned with the organisation's needs.

2.12 Conclusion

The huge growth in digital data and the commoditisation of personal information has brought privacy to the forefront of world, and South African, legislation. The impact and growth of the internet, digitisation of data, network connectivity and data sharing has required that new threats be addressed. PoPI lists a number of privacy commitments that South African organisations will need to attend to: *transparency* in the form of clear communications with clients, *respect* of people's personal information, a data subject's *choice* of whether their personal information can be shared, the *accountability* of users of personal data, and ensuring that *privacy design* is part of any new initiative, product or service and *complies* with regulatory requirements.

The impact of PoPI is multi-disciplinary, industry agnostic, blind to organisation size and will touch both the public and private sectors. Government institutions like schools and hospitals which store large amounts of personal data, the financial industry which uses personal information to grant loans for housing, investment and motor finance, marketing and sales organisations who use personal information as a profiling tool for commercial appeal, will require PoPI compliance.

Due to PoPI impacting on technical controls, processes and human resources within an organisation, the requirements to become PoPI compliant will rely on revising:

- Legal and compliance management;
- Human resources management;
- Information governance;
- Information security;
- Records management;
- Business continuation planning;
- Third party service provider management.

By updating the above-mentioned controls and aligning them with PoPI, an organisation will take the first proactive steps in developing an overall information privacy management program. Utilising global best practice frameworks and standards for privacy and technical controls (ISO 27001/2 for example) can provide an organisation with a valuable starting point when addressing this type of program.

The next chapter introduces the design science research methodology undertaken for this dissertation and presents the development cycle undertaken to produce the artefact in this research.

3. RESEARCH METHODOLOGY

The purpose of this chapter is to explore design science and how it can be used to create an artefact used in measuring an organisation's privacy maturity in relation to best practice and the PoPI Act. The intention is to break down the design science methodology and explain the benefits of using an iterative building process when dealing with artefact design, especially where the "problems are inherently wicked" (Rittel & Webber, 1973, p. 160) and require an understanding of all the possible available solutions.

3.1 Research Design

The Cambridge Dictionary defines research as "a detailed study of a subject, especially in order to discover (new) information or reach a (new) understanding" (Cambridge Advanced Learner's Dictionary & Thesaurus, 2013). Marczyk, DeMatteo and Festinger (2005) define research as an attempt "to reduce the complexity of problems, discover the relationship between seemingly unrelated events, and ultimately improve the way we live" (p. 1). This provides a close correlation to design science's approach of "creating new and innovative artefacts...to extend the boundaries of human and organizational capabilities" (Hevner, March, Park, & Ram, 2004, p. 75).

Design science has its roots in engineering where design "is concerned with how things ought to be, with devising artefacts to attain goals" (Simon, 1996, p. 114). Design science is essentially a problem solving paradigm seeking "to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis,design, implementation, management, and use of information systems can be effectively and efficiently accomplished" (Hevner et al., 2004, p. 76).

Considering the complex interactions associated with the real-world problem of PoPI compliance, and the human creativity required to design a suitable artefact (Hevner et al., 2004), the problem posed in this research is typical of a design science project.

3.2 Research Philosophy

The importance of the researcher's basic beliefs of the world (theoretical perspective) forms an integral part in the direction of this research project. Before presenting the philosophical grounding of design science and the direction of this research, it is worth providing definitions of the philosophical assumptions:

Ontology is the study that describes the nature of reality: for example, what is real and what is not, what is fundamental and what is derivative?

Epistemology is the study that explores the nature of knowledge: for example, on what does knowledge depend and how can we be certain of what we know?

Axiology is the study of values: what values does an individual or group hold and why?

At a philosophical level two primary research paradigms exist: positivism and interpretivism. While these two paradigms exist at the polar ends of the philosophical continuum (Collins & Hussey, 2003) the researcher's beliefs lie somewhere in-between.

The positivist paradigm is based on scientific observation and empirical inquiry (Gray, 2009) believing that the world exists independently of the researcher (Collins & Hussey, 2003), and that the researcher should use objective methods and conclusions when making observations (Creswell, 2013). Contrasting this paradigm, interpretivism "is concerned with understanding human behaviour from the participant's own frame of reference" (Collins & Hussey, 2003, p. 53). Due to the researcher's own experiences, and being part of the observed reality (Collins & Hussey, 2003), the truth is interpreted by investigating our social experiences of reality (Gray, 2009).

Creswell (2013) states that we cannot claim facts and absolute truths when studying the behaviour and actions of humans, and Mingers (1997) suggests that a multiplicity of methodologies can be utilised because 1) any situation is complex and no single methodology can tackle it completely, and 2) an intervention is not a discreet event but falls on a continuous timeline and therefore different methodologies may be more applicable at different stages of the intervention. Lane and Silva (as cited in Harrop,

Gillies, & Wood-Harper, 2012) contend that a synthesis of positivism with interpretivism translates positivist concepts to an interpretivist paradigm. Post-positivism emerges as a paradigm closely aligned with this research as it presents a refined version of positivism by establishing that we cannot claim facts and absolute truth when studying the behaviour and actions of humans (Creswell, 2013).

While a post-positivist perspective is adopted for this research, design science provides the most accurate philosophical description. Baskerville (2008) argues that design science is more of a research paradigm than a research methodology as it changes the state of the world through the development of purpose-driven artefacts. Vaishnavi and Kuechler (2004) propose that the philosophical grounding of a design science researcher changes as the design science project progresses. The creation of a new reality is provided by the observation and interpretation of the results from the constructed intervention.

Gregg, Kulkarni and Vinzé (2001) provide a summary (Table 5) of the philosophical assumptions of the three "ways of knowing" with the addition of the axiology provided by Vaishnavi and Kuechler (2004).

Table 5: Philosophical assumptions of three research perspectives (Gregg et al., 2001)

	Research Perspective		
Basic Belief	**Positivist**	**Interpretive**	**Design**
Ontology	A single reality. Knowable, probabilistic	Multiple realities, socially constructed	Multiple, contextually situated alternative world-states. Socio-technologically enabled
Epistemology	Objective; dispassionate. Detached observer of truth	Subjective, i.e. values and knowledge emerge from the researcher-participant interaction.	Knowing through making: objectively constrained construction within a context. Iterative circumscription reveals meaning
Methodology	Observation; quantitative, statistical	Participation; qualitative. Hermeneutical, dialectical.	Developmental. Measure artefactual impacts on the composite system.
Axiology	Truth: universal and beautiful; prediction	Understanding: situated and description.	Control; creation; progress (i.e. improvement); understanding

3.3 Research Approach

According to March and Smith (1995) design science consists of two principle actions namely, build and evaluate. The build phase is concerned with constructing an artefact that addresses a problem, while the evaluation phase measures the artefact's performance. Both Hevner's (2007) "design science research cycles" (Figure 1) and Vaishnavi and Kuechler Jr's (2007) "general design cycle" (Figure 2) illustrate the build and evaluate process within design science.

All design begins with a problem or opportunity and the identification, or awareness, that a solution can be developed. The development, or design science stage provides for the creation of an artefact. An iterative design and evaluation process offers feedback to the expected results of the artefact, and provides rigour to the development cycle. Due to the interdisciplinary nature of this study (law and IT) the evaluation process will include expert opinions from both fields. The conclusion of the process (cycle) should result in a purposeful IT artefact presented to a wide audience (Hevner et al., 2004).

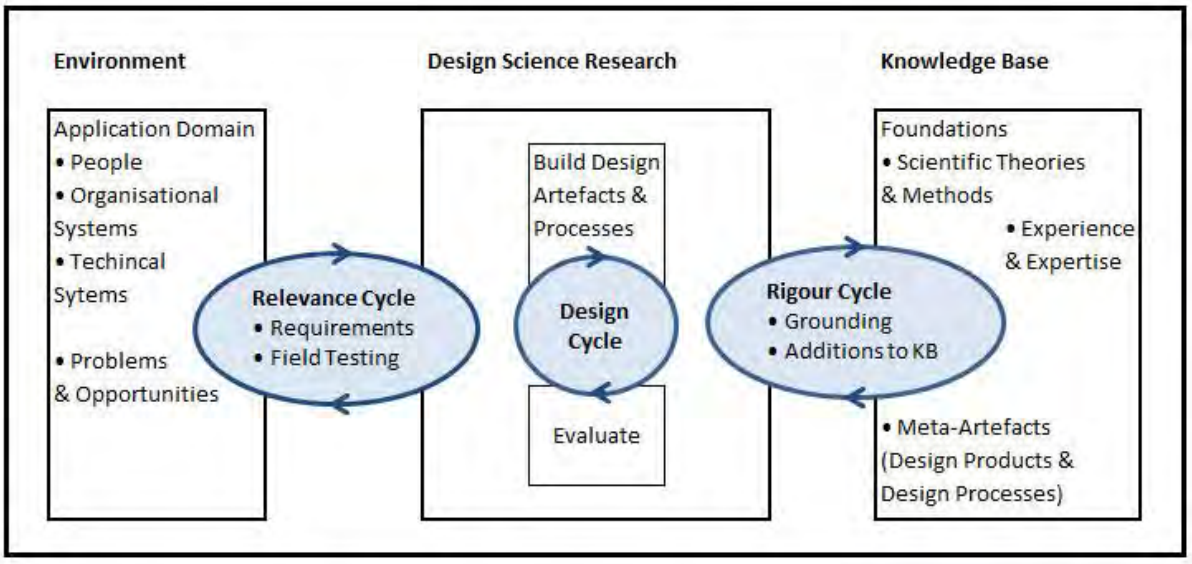

Figure 1: Design-science research cycles (Hevner, 2007)

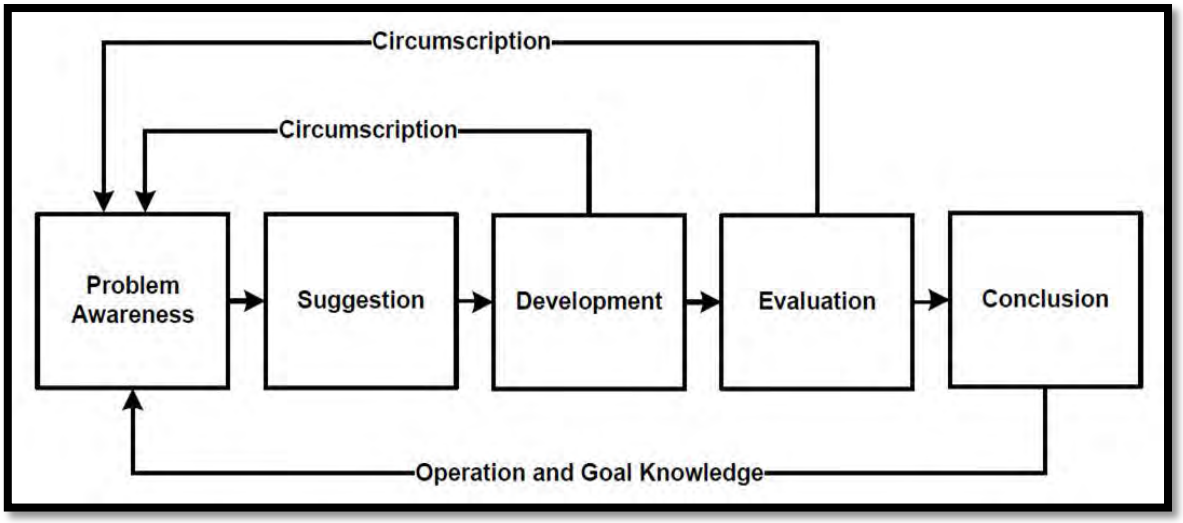

Figure 2: General design cycle (Vaishnavi & Kuechler Jr, 2007)

Besides the final product of a purposeful IT artefact described by Hevner (2007), March and Smith (1995) propose that four artefacts are produced from design science research:

Constructs: The vocabulary used to define the problem/solution domain. The language used to conceptualise the problem and to specify their solutions. Constructs constantly evolve and are refined during the research process.

Models: "Is a set of propositions or statements expressing relationships among constructs" (March & Smith, 1995, p. 256). They are proposals for how things are or should be (Vaishnavi & Kuechler, 2004).

Methods: Based on the underlying constructs and model, this is the "how-to knowledge" of arriving at a solution. "A method is a set of steps (an algorithm or guideline) used to perform a task" (March & Smith, 1995, p. 257).

Instantiations: This is the final output from design science research and demonstrates "the feasibility and effectiveness of the models and methods they contain" (March & Smith, 1995, p. 258). The *instantiation* of an artefact in essence operationalises constructs, models and methods (Vaishnavi & Kuechler, 2004).

March and Smith's (1995) framework provides for the generation of an artefact at each design stage based on the knowledge from the preceding output. Figure 3 illustrates the design science research outputs according to Smith and March.

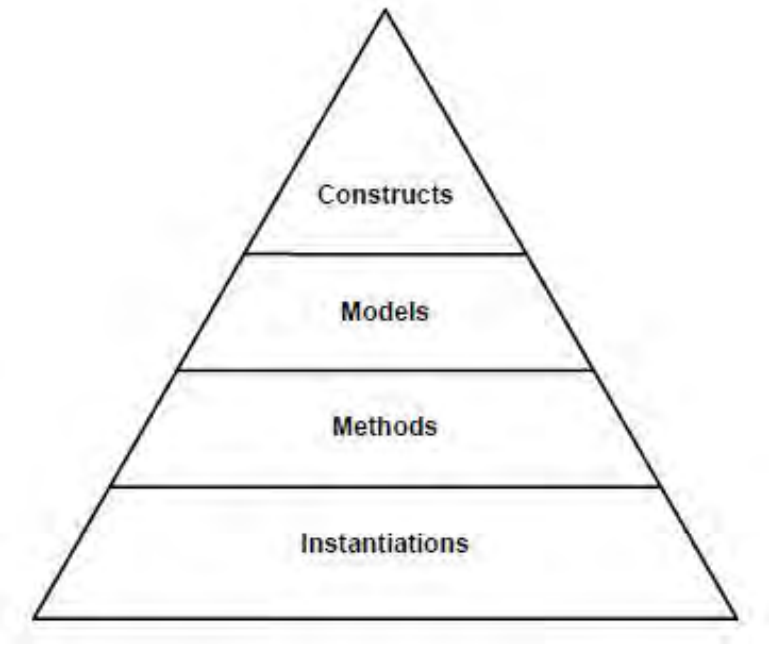

Figure 3: Design science artefacts

In addition to the four constructs outlined by March and Smith (1995), Vaishnavi and Kuechler Jr. (2007) propose a fifth artefact as output, referred to as "better theories" (p. 14). These better theories can be produced in two ways: 1) through the methodological construction of artefacts, or 2) through the exposure of the relationships between the elements of an artefact (Manson, 2006). Utilising Vaishnavi and Kuechler Jr's (2007) General Design Cycle (Figure 2 above) the iterative, or circumscription process of design science, provides for the artefact construction or exposure of the relationships between the elements of the artefact. They emphasize that "the circumscription process is especially important in understanding design science research because it generates understanding that could only be gained from the specific act of construction" (Vaishnavi & Kuechler Jr, 2007, p. 12).

3.4 Design Science Requirements

On the completion of an artefact it is important to ensure that it complies with accepted design science practice. Hevner et al. (2004) establish seven requirements for comparative purposes:

1. *Design as an artefact:* the creation of an innovative, purposeful artefact.
2. *Problem relevance:* The design must address a relevant and important problem.
3. *Design evaluation:* it must yield utility for the specified problem (thorough/rigourous evaluation of the artefact is crucial).
4. *Research contributions:* the artefact must be novel and innovative, solving a new problem, or providing a more effective or efficient solution.
5. *Research rigour:* research methods must be rigorously defined, formally represented, coherent, and internally consistent.
6. *Design as a search process*: an iterative or cyclical problem solving process should be used.
7. *Communication of research*: research must be communicated effectively to a wide audience; results need to address the rigourous requirements of academia as well as relevance for a professional audience.

While Hevner et al. (2004) provide these guidelines to assist researchers, they advise against taking a mandatory, or rote, use of them, instead to utilise “creative skills and judgment” (p. 82) to determine when, where and how to apply each guideline.

The overall aim of this research is the development of a *model*. However, due to the stage-based development process it is envisaged that artefacts within the *construct* and *method* stages will also be developed, while *instantiation* will follow naturally through the evaluation process.

3.5 Ethics and Confidentiality

This research followed the six ethical principles outlined by Myers and Venable (2014) for design science research as outlined in Table 6 below:

Table 6: Ethical principles for design science research (Myers and Venable, 2014)

Ethical Principle	This Research
Public Interest	The artefact as has been developed as an assessment tool. All stakeholders involved in the development, design and testing phases were aware that the finished product would in no way provide compliance with PoPI.
Informed Consent	Both evaluators provided consent.
Privacy	All personally identifiable information has been removed and anonymity has been ensured.
Honesty and Accuracy	Accuracy has been achieved through development design cycle and the rigorous review by industry experts. Honesty is mandated by the UCT research and ethics codes undertaken by this research.
Property	All IP, or ownership of the artefact is covered by UCT polices which have been abided by.
Quality of Artefact	The quality of the artefact is assured through the involvement of industry experts who were part of the review process. This artefact is of low risk as it is an assessment tool and makes no claims about compliance.

3.6 Conclusion

Utilising the cyclical development methodology of design science, and following the seven compliance principles outlined by Hevner et al. (2004), this dissertation intends to develop an artefact based on the criteria outlined for a model. The next chapter provides an in-depth overview of maturity models and the importance they play in the development of the model for this dissertation.

4. MATURITY MODELS

Due to the importance maturity models play as a construct within the development of the artefact as both a problem domain and solution, it is important to understand this process before outlining the conceptual model in Chapter 5.

Over twenty years ago the Software Engineering Institute launched the Capability Maturity Model (CMM) (Paulk, Curtis, Chrissis, & Weber, 1993) which precipitated hundreds of maturity models across multiple domains by researchers and practitioners (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005; Weber, Curtis, & Gardiner, 2008). Maturity models have been developed to assist organisations within digital government (Gottschalk, 2009), IT management (Becker, Knackstedt, & Pöppelbuß, 2009; IT Governance Institute, 2014), knowledge management (Kulkarni & Freeze, 2004), and business process management (Hammer, 2007; Weber et al., 2008), and the trend is expected to increase (Scott, 2007) as businesses strive for continuous process improvement.

4.1 The Purpose of Maturity Models

The continual pressure faced by organisations to gain and retain competitive advantage by identifying ways to cut costs, improve quality and reduce time to market has resulted in the development of maturity models (De Bruin et al., 2005). These models are used as an evaluative and comparative basis for improvement (Fisher, 2004; Harmon, 2004; Spanyi, 2004) within an organisation, with the view of providing an informed decision for increasing the capability within a specific area of the business (Ahern, Clouse, & Turner, 2004; Hakes, Popplewell, Gallacher, & Clements, 1995; Paulk et al., 1993). Maturity models have been designed to assess the maturity (i.e. competency, capability, level of sophistication) of a selected area within an organisation based on a set of criteria (De Bruin et al., 2005) with the intention to diagnose and eliminate deficient capabilities (Rummler & Brache, 2012).

While maturity models offer a method for assessing an organisation’s capability they have been the subject of criticism since their inception. The step-by-step measurement process has been considered an oversimplification of reality as well as lacking in empirical foundation (Benbasat, Dexter, Drury, & Goldstein, 1984; De Bruin et al., 2005; King & Kraemer, 1984; McCormack et al., 2009). Furthermore,

Teo and King (1997) suggest that maturity models tend to disregard the possibility of multiple equally beneficial paths. Due to the possibility of multiple paths, King and Kraemer (1984) theorise that maturity models should place more value on the factors driving evolution and change in place of a sequence of levels driving towards a predefined “end state”.

Although the criticism of maturity models paints them as limiting, Rummler & Brache (2012, p. 25) describe tools of this nature as an engine for continuously improving systems, roadmaps for guiding organisations, and blueprints for designing new entities. Outside of the metaphorical descriptions of maturity models, the following purposes have more practical implementations:

- *Descriptive*: where the purpose of the model is to describe an “as-is” assessment of an organisation’s current capabilities based on a set of given criteria (Becker et al., 2009) and is used as a diagonostic tool (Maier, Moultrie, & Clarkson, 2009) to assign maturity levels for reporting to the relevant stakeholders;
- *Prescriptive*: where the model provides “specific and detailed courses of action” (Maier et al., 2009, p. 21) and indicates desirable maturity levels with guidelines on achieving those levels (Becker et al., 2009);
- *Comparative*: based on historical data from prior asessments in similar business units or organisations, models offer a comparative purpose based on matuirty levels achieved (De Bruin et al., 2005; Maier et al., 2009).

4.2 Concepts and Approaches to Maturity

“The basic concept underlying maturity is that mature organizations do things systematically while immature organizations achieve their outcomes as a result of the heroic efforts of individuals using approaches that they create more or less spontaneously” (Harmon, 2004, p. 1). The systematic development of process maturity is based on the assumption of predicatable patterns and the evolution of business capabilties in a stage-by-stage manner along an antipicated maturation path (Gottschalk, 2009). This requires the measurement of various “levers of change” (Fisher, 2004) - people, processes or technology for example, within a business.

As the CMM has gained global acceptance as a maturity model (De Bruin et al., 2005), and is considered the blueprint of current maturity models, it follows that the most popular evaluation method is via a five-point Likert scale (with "5" representing the highest level of maturity). While the terminology may differ between various maturity models (Table 7), the concept of incremental maturity levels remains similar (Figure 4).

Table 7: Comparative maturity models

Maturity Model	Level 1	Level 2	Level 3	Level 4	Level 5
Capability Maturity Model	Initial	RepeaTable	Defined	Managed	Optimising
Center for Business Practices	Initial process	Structure Process and Standards	Organisational Standards and Institutionalised Project Management	Managed	Optimising
Project Management Maturity Model	Common Language	Common Processes	Singular Methodology	Benchmarking	Continuous Improvement
Berkley Model	Ad hoc	Planned	Managed at Project Level	Managed at Corporate Level	Learning
ESI International's Project Framework	Ad hoc	Consistent	Integrated	Comprehensive	Optimising

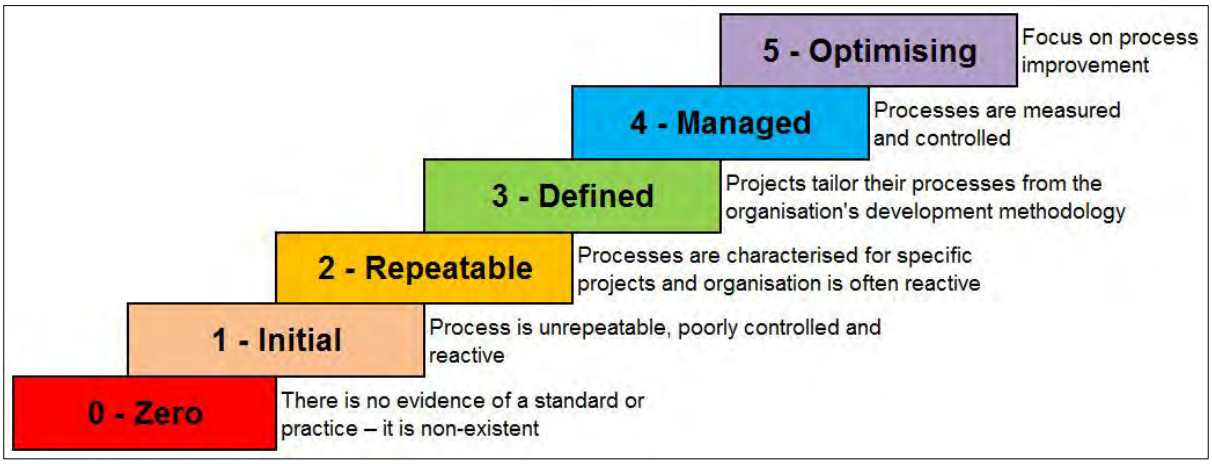

Figure 4: Incremental maturity levels as per the CMM

Using the CMM as an example, the characterisations in Table 8 can be attributed to the five maturity levels (Axelos, 2013).

Table 8: CMM maturity levels (Axelos, 2013)

Level	Description	Definition
1	Initial	Procedures or processes are generally informal, incomplete and inconsistently applied. While there is evidence an organisation has recognised that issues exist and need to be addressed, there are no standardised procedures in place, and the process/function is regarded as of minor importance, with few resources allocated to it. Instead, ad hoc approaches tend to be applied on an individual or case-by-case basis, and the overall approach is disorganised.
2	Repeatable	Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects, although they follow a regular pattern. Similar procedures are followed by different people undertaking the same task, however, there is no communication of standard procedures, and responsibility is left to the individual. This leads to the reliance on individual knowledge and therefore errors are likely. In general, activities related to the process or functions are uncoordinated, irregular and directed towards process or function efficiency.
3	Defined	Procedures and processes are fully standardised, documented and implemented, and cover all relevant aspects. While the procedures may not be sophisticated, they have been formalised from existing practices, although it is left to individuals to follow these procedures and deviations may occur. Processes have a process owner, formal objectives, targets, allocated resources, and are focused towards both efficiency and effectiveness therefore becoming more proactive and less reactive.
4	Managed	Processes are service-focused and have objectives and targets that are aligned with business objectives and goals. Reviews are conducted to assess the effectiveness of the controls in place and processes and functions are monitored and measured for compliance. Action is taken where processes or functions appear not to be working effectively and constant improvement is enforced with automation increasingly used to deliver efficient operations.
5	Optimised	Best practices are followed and automated and regular reviews and feedback are used to ensure continuous improvement towards optimisation of the given process. The process or function has strategic objectives and goals aligned with overall strategic business goals and have become institutionalised as a business as usual strategy.

4.3 The Design of Maturity Models

The evolutionary process outlined by a typical maturity model follows a similar pattern to the development of the maturity model itself. Some IS researchers (e.g., Becker et al., 2009; Mettler & Rohner, 2009) view the development of maturity models in line with the design science methodology. Design science research seeks to create innovative artefacts that are useful for coping with human and

organisational challenges (Hevner et al., 2004). Based on the design science categories given by March and Smith (1995), Mettler and Rohner (2009) question which artefact type a maturity model would represent. The suggestion is that maturity models are “some-how in-between” (Mettler & Rohner, 2009, p. 2) models and methods due to combining descriptions (i.e., *models* of distinct maturity levels) with activities (i.e., *methods* for conducting assessments, recognising need for action, and selecting improvement measures).

The evaluation of artefacts is an essential part of design science research (Hevner et al., 2004; March & Smith, 1995). Supposed to be innovative and useful, artefacts are commonly evaluated “with respect to the utility provided for the class of problems addressed” (Hevner et al., 2004, p. 77). The three practical applications of maturity models mentioned above, namely descriptive, prescriptive and comparative, while considered distinct, are deemed to follow an evolutionary development cycle (De Bruin et al., 2005). A model begins descriptively to provide a deeper understanding of an organisations current “as-is” capabilities. From this initial stage the model can develop into a more prescriptive tool offering guidelines, or detailed actions, leading to repeatable improvements and improved maturity levels. Finally, for a model to be used comparatively “it must be applied in a wide range of organisations in order to attain sufficient data to enable valid comparison” (De Bruin et al., 2005, p. 3).

The *qualities* and *components* required to build a maturity model through design science need consideration. Moody and Shanks (1994) identify qualities as representing the desirable properties or dimensions of value, while the components shape a maturity model’s structure. General qualities such as correctness, relevance, flexibility, understandability, implementability, and economic efficiency (Pöppelbuß & Röglinger, 2011) should be considered, while more maturity model specific criteria such as validity, reliability, cost efficiency (Simonsson, Johnson, & Wijkström, 2007), benchmarking applicability, certification, and disclosure of potential for improvement should be included. Having identified the qualities of a maturity model Fraser, Moultrie and Gregory (2002) suggest the following components: levels, descriptors, descriptions for each level, dimensions, process areas, activities for each process area, and a description of each activity as performed at a certain maturity level.

The design process of maturity models using design science principles has taken different forms with De Bruin et al. (2005) proposing six phases to guide the design of a maturity model through the descriptive, prescriptive and finally comparative models (Figure 5). Becker et al. (2009) utilise Hevner et al.'s (2004) design science guidelines to distinguish eight phases that provide "a manual for the theoretically founded development and evaluation of maturity models" (Becker et al., 2009, p. 221).

Figure 5: Model development phases (De Bruin et al., 2005)

Pöppelbuß and Röglinger (2011) consider both De Bruin et al (2005) and Becker et al.'s (2009) models important from a structural perspective, and extend these frameworks by adding three layers of design principles (Figure 6). The objective is to define general design principles of form and function which maturity models should comply to for them to be used effectively in their applicable domain and for their designated purpose.

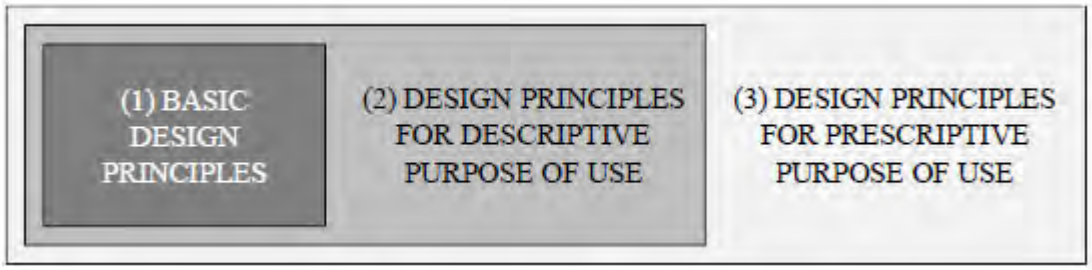

Figure 6: Organisation design principle framework (Pöppelbuß & Röglinger, 2011)

4.4 Conclusion

Maturity models have been designed to assess the maturity of a selected area within an organisation based on a set of criteria (De Bruin et al., 2005) with the intention to diagnose and eliminate deficient capabilities (Rummler & Brache, 2012), and this is no different when assessing an organisation's privacy maturity levels.

The PoPI Act presents privacy as the rights and obligations of individuals and organisations with respect to the collection, use, retention, disclosure, and disposal of personal information. These privacy considerations become significant in light of the new legislation for organisations that collect, use, retain and disclose personal information about customers, employees and others.

Becoming privacy compliant is a process, and to facilitate this the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) developed tools, processes and guidance based on Generally Accepted Privacy Principles (GAPP) to assist organisations in strengthening their privacy policies, procedures and practices.

Chapter 5 examines both the GAPP framework and related privacy maturity model as constructs in the foundation for this dissertation's conceptual model.

5. CONCEPTUAL FOUNDATION

This chapter develops the model referred to as the PoPI Privacy Maturity Model (PoPI-PMM), utilised in measuring an organisation's potential readiness with regards to the PoPI act. March and Smith (1995) define a model as "a set of propositions or statements expressing relationships among constructs. In design activities, models represent situations as problem and solution statements" (p. 256). The model is prescriptive in that it provides the building blocks from which an implementation can be developed. These building blocks are drawn from instantiations of a (privacy) maturity model, relevant best practices, as well as the newly enacted PoPI Act (2013). This chapter provides a conceptual overview of the model, while the following chapter outlines the functional instantiation of the PoPI-PMM.

5.1 Scope of the Model

Vaishnavi and Kuechler Jr. (2007) suggest several patterns to produce an effective solution using design science, and this model utilises a hierarchical design pattern. The intent of a hierarchical design pattern is to create a complex artefact by designing smaller, simpler subsystems therefore reducing the overall complexity of design – a "divide and conquer strategy" (Vaishnavi & Kuechler Jr, 2007, p. 136).

Figure 7 shows the four subsystems utilised to create the final PoPI-PMM:

- CICA / AICPA: using the CICA/AICPA privacy maturity model and generally accepted privacy principles as a best practice framework for the new models foundation;
- Maturity Assessment: utilising the ITIL maturity model and assessment service to provide a practical overview in terms of processes, policies, business objectives, process improvements and benchmarking;
- PoPI: mapping the relevant PoPI sections to the privacy maturity framework to provide a tool within the South African context;
- Risk Weighting: identifying risk areas within a business that will highlight any potential heightened privacy issues.

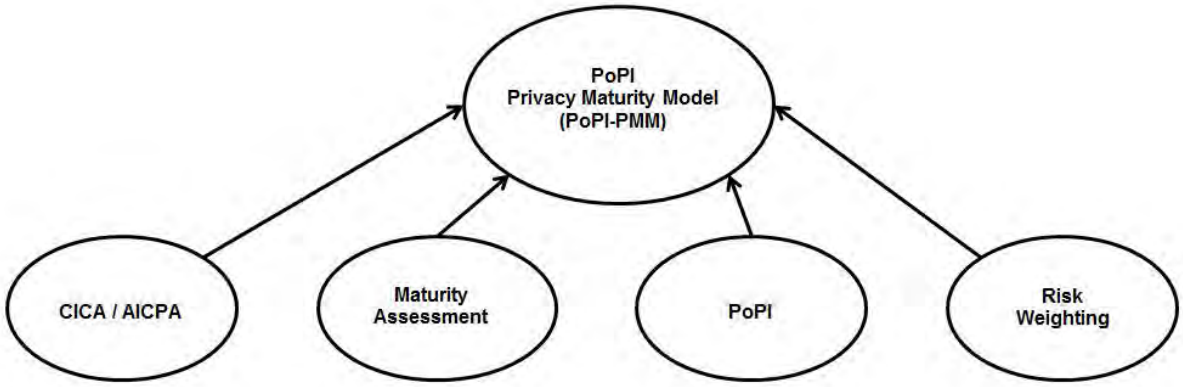

Figure 7: Functional scope of the model

In line with design science nomenclature the subsystems are referred to as constructs, and as stated by March and Smith (1995), a model is “a set of propositions or statements expressing relationships among constructs” (p. 256). The following sections provide a more detailed definition of the model and define the key constructs and their relationships.

5.2 Construct 1: CICA / AICPA

The PoPI-PMM is grounded in the Generally Accepted Privacy Principles (GAPP) and Privacy Maturity Model (PMM) developed by a taskforce comprising members from both the Canadian Institute of Chartered Accountants (CICA) and American Institute of Certified Public Accountants (AICPA). GAPP was developed as a tool to assist Certified Public Accountants (CPAs) in offering clients a range of services, including privacy strategic and business planning; privacy gap and risk analysis; privacy policy design and implementation; and independent verification of privacy controls, which includes attestation engagements (Harden, 2007). GAPP is considered one of the most comprehensive privacy governance frameworks (Dennedy, Fox, & Finneran, 2014) and was designed to encompass the key points of various existing frameworks as seen in Table 9 below:

Table 9: Key privacy framework alignment (Dennedy, Fox, & Finneran, 2014, p. 57)

GAPP	OECD Guidelines	FTC FIPPS	EU Directive	ISO 27002	APEC
Management				Operations management	Preventing Harm
Collection	Collection limitation		Proportionality	Information acquisition	Collection limitations
Quality	Data quality				Integrity of personal information
Notice	Specification of purpose	Notice / awareness	Transparency		Notice
Use, retention, disposal	Use limitation		Legitimate purpose	Asset management	Use of personal information
Security for privacy	Security safeguards	Integrity / security		Security	Security safeguards
Access	Openness	Access / participation		Access control	Access and correction
Choice / consent	Individual participation	Choice / consent		Asset management	Choice
Moniotoring and enforcement	Accountability	Enforcement / redress	Supervisory authority	Compliance	Accountability
Disclosure to third parties			Transfer of personal data to third parties		

According to AICPA and CICA who jointly developed the Generally Accepted Privacy Principles (AICPA/CICA, 2011, p. 1):

> *Generally Accepted Privacy Principles has been developed from a business perspective, referencing some but by no means all significant local, national and international privacy regulations. GAPP converts complex privacy requirements into a single privacy objective supported by 10 privacy principles. Each principle is supported by objective, measurable criteria (73 in all) that form the basis for effective management of privacy risk and compliance. Illustrative policy requirements, communications and controls, including their monitoring, are provided as support for the criteria.*

The ten GAPP principles comprise:

Table 10: Generally accepted privacy principles (CICA/AICPA, 2009)

No.	Principle	Description
1.0	Management	The organisation defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2.0	Notice	The organisation provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3.0	Choice and Consent	The organisation describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4.0	Collection	The organisation collects personal information only for the purposes identified in the notice.
5.0	Use and Retention	The organisation limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The organisation retains personal information for only as long as necessary to fulfill the stated purposes.
6.0	Access	The organisation provides individuals with access to their personal information for review and update.
7.0	Disclosure to Third Parties	The organisation discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8.0	Security for Privacy	The organisation protects personal information against unauthorised access.
9.0	Quality	The organisation maintains accurate, complete and relevant personal information for the purposes identified in the notice.
10.0	Monitoring and Enforcement	The organisation monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Each privacy principle is supported by objective, measurable criteria (73 in total) that form the basis for effective management of privacy risk and compliance in an organisation (Schroeder, 2011). Figure 8 outlines the generic breakdown of the GAPP principles and the associated controls:

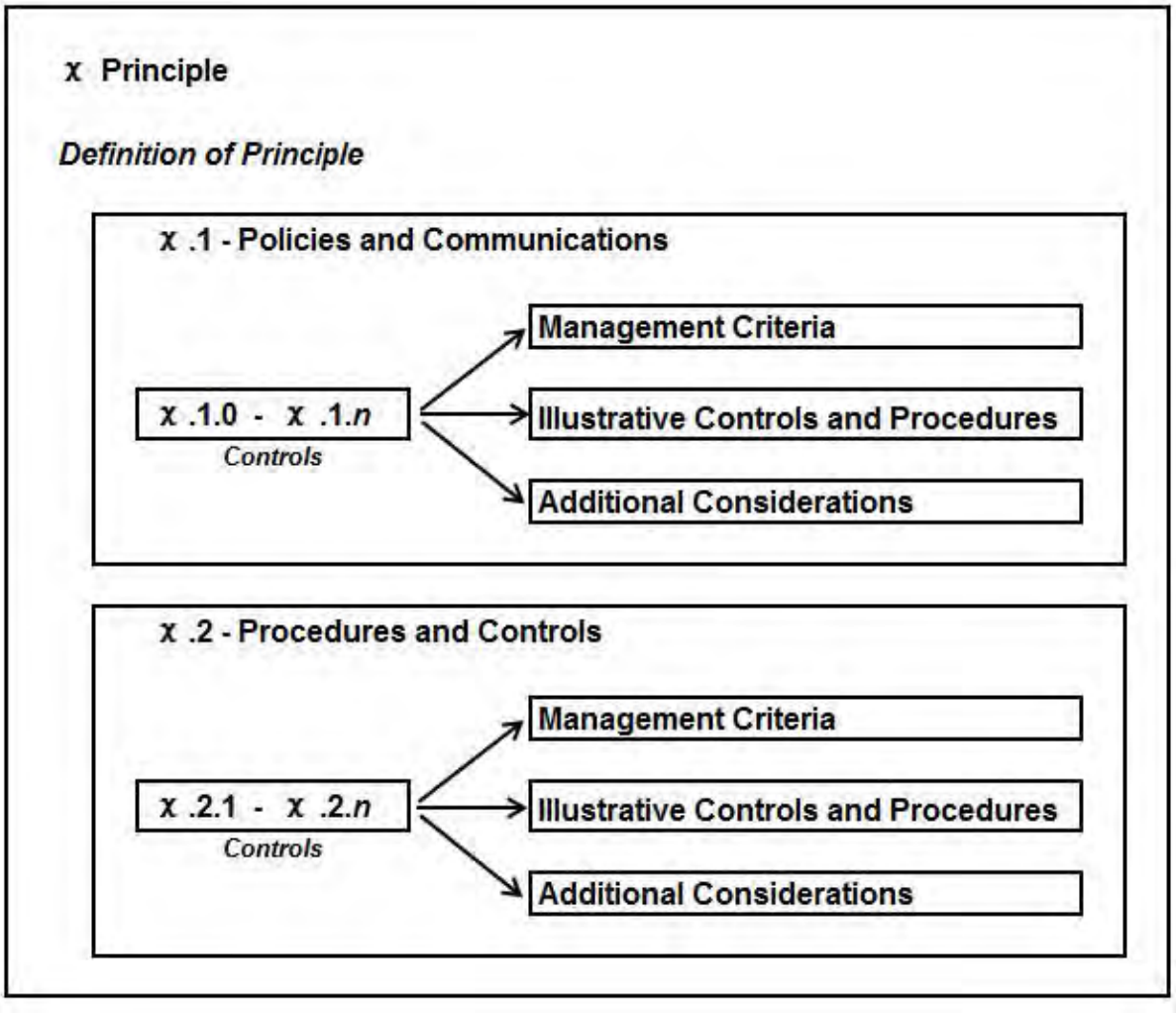

Figure 8: Generic GAPP breakdown

Table 11 provides a sample of the how the GAPP criteria are defined as management criteria with the associated illustrative controls and procedures:

Table 11: GAPP criteria

Management Criteria	Illustrative Controls and Procedures
1.2.2 Consistency of Privacy Policies and Procedures with Laws and Regulations Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Corporate counsel or the legal department: • Determines which privacy laws and regulations are applicable in the jurisdictions in which the entity operates. • Identifies other standards applicable to the entity. • Reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws, regulations and appropriate standards.

The CICA/AICPA extended GAPP by developing the Privacy Maturity Model (PMM) which is based on the ten GAPP principles and the CMM. Each of the 73 GAPP criteria can be assigned a value from 1 to 5 representing a level of maturity based on the CMM (refer Table 7 in Chapter 4).

The GAPP and PMM frameworks fit together and form the foundation to the PoPI-PMM tool (illustrated in Figure 9). The 73 criteria cover ten GAPP principles which encompass the framework's elements of privacy. Using the five levels of maturity established by the CMM framework as a "wrapper" around the GAPP principles, allows for the development of the Privacy Maturity Model.

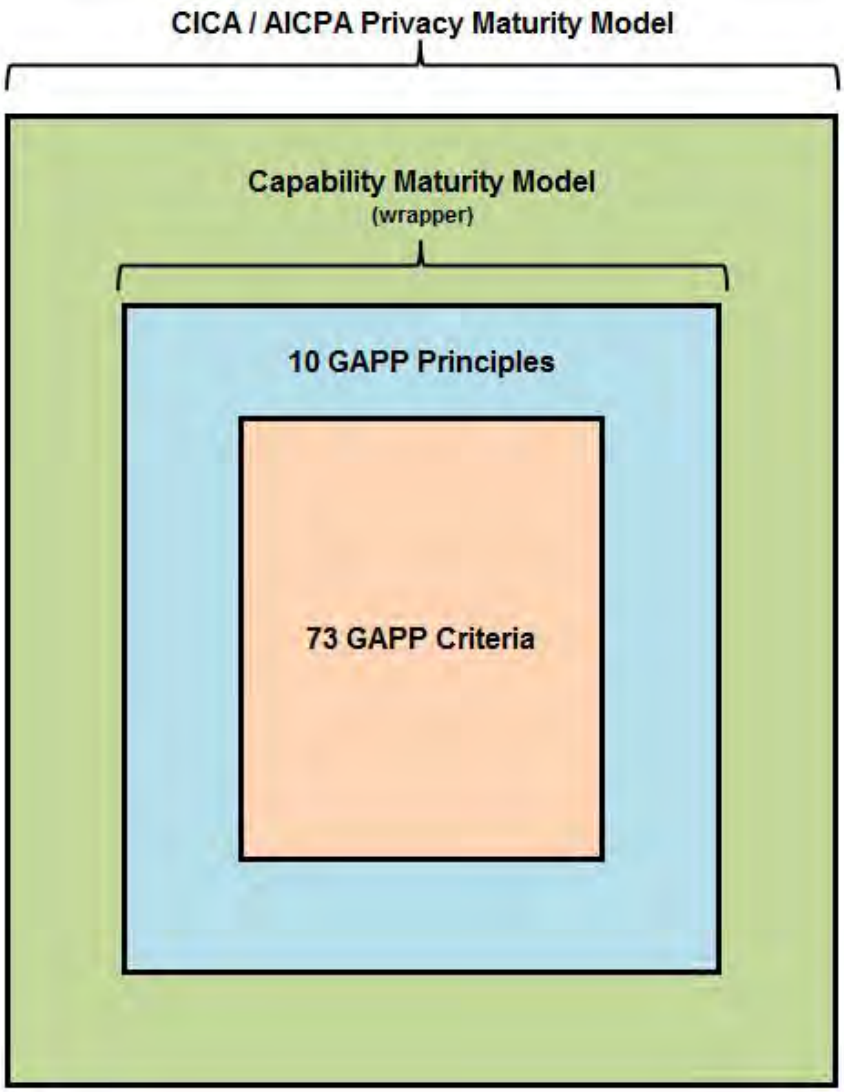

Figure 9: CICA/AICPA GAPP and PMM framework

The first stage in the development of the PoPI-PMM is to break GAPP into its constituent parts – 73 GAPP criteria grouped within the ten principles (Figure 10, full breakdown in Appendix D).

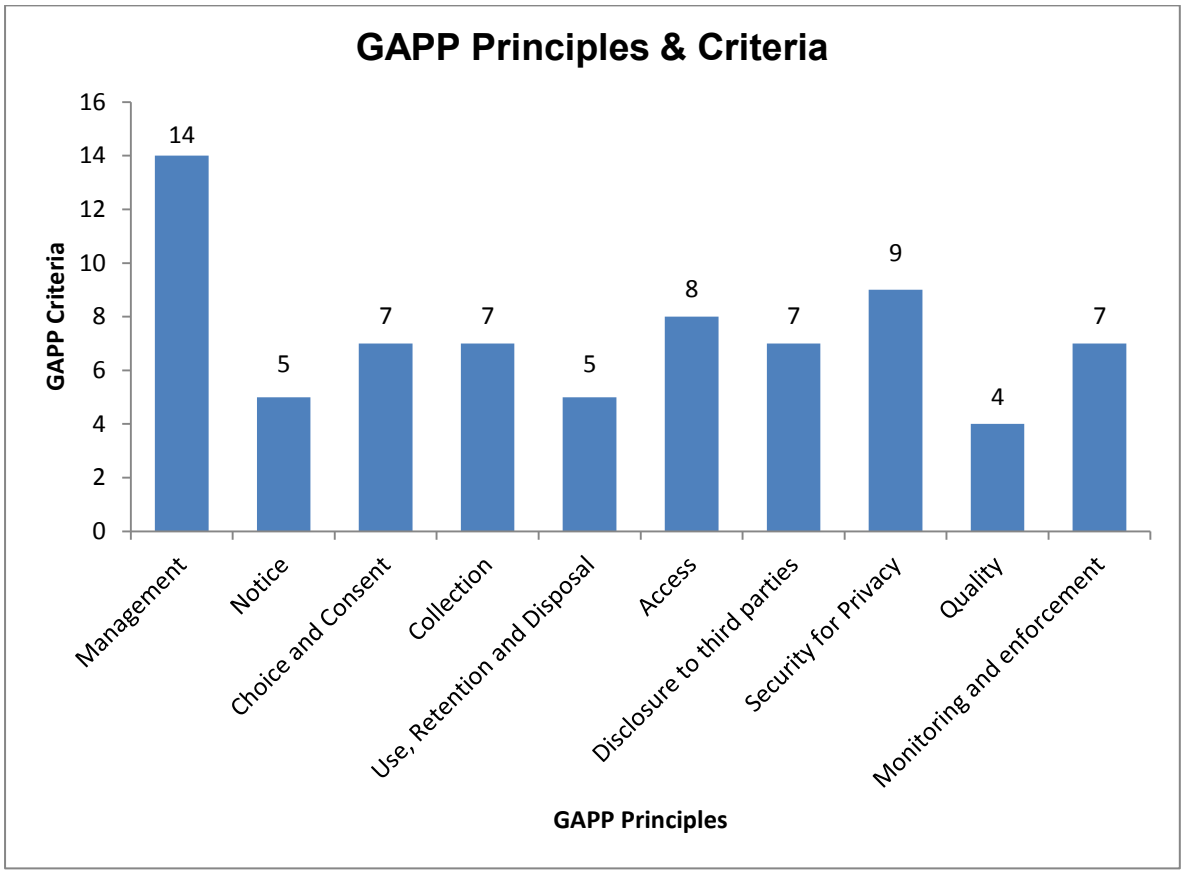

Figure 10: GAPP Principles and criteria

5.3 Construct 2: Maturity Assessment

Having separated GAPP into its constituent parts, the second process is to assess the maturity of the 73 GAPP criteria. While the CMM uses a ranking scale from one to five, the PoPI-PMM includes zero as a starting value as this represents cases where there is no evidence of a standard or practice existing (Figure 11). Using a scale from zero to five an organisation is able to assess the maturity of each GAPP criterion and calculate an overall assessed maturity level for a Principle.

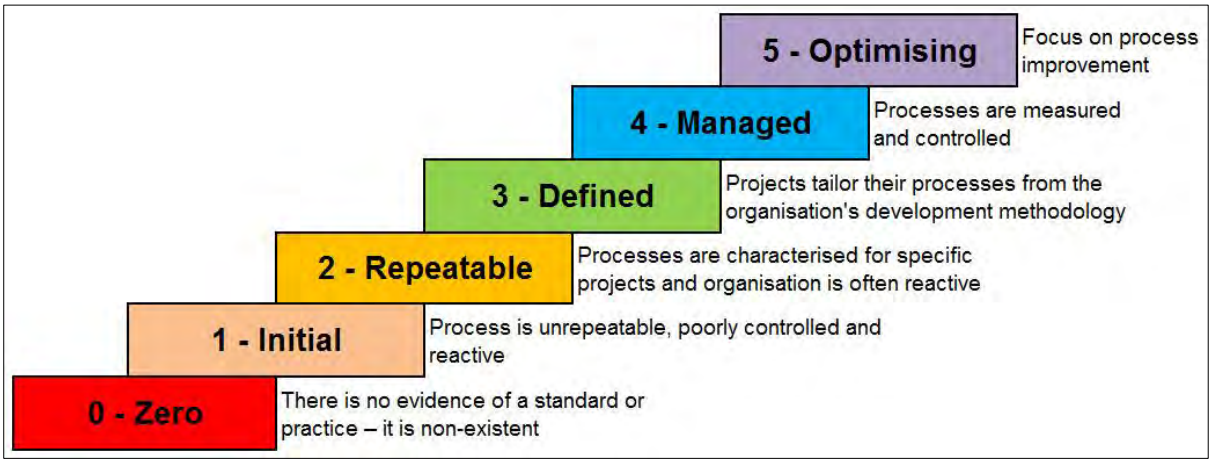

Figure 11: Extended CMM maturity levels

The process of calculating the *assessed Principle maturity level* (M) begins by applying a rating value from zero to five to each GAPP *criteria* (C) within a Principle. Once all the criteria within a Principle have been allocated a value, these are then summed and averaged by the number of criteria within the Principle:

$$M = \sum C / count(C)$$

The resulting value provides an organisation with a view of how mature they are for each of the ten generally accepted privacy principles. Figure 12 provides an example of how the modified CMM ranking process could be represented in practical terms.

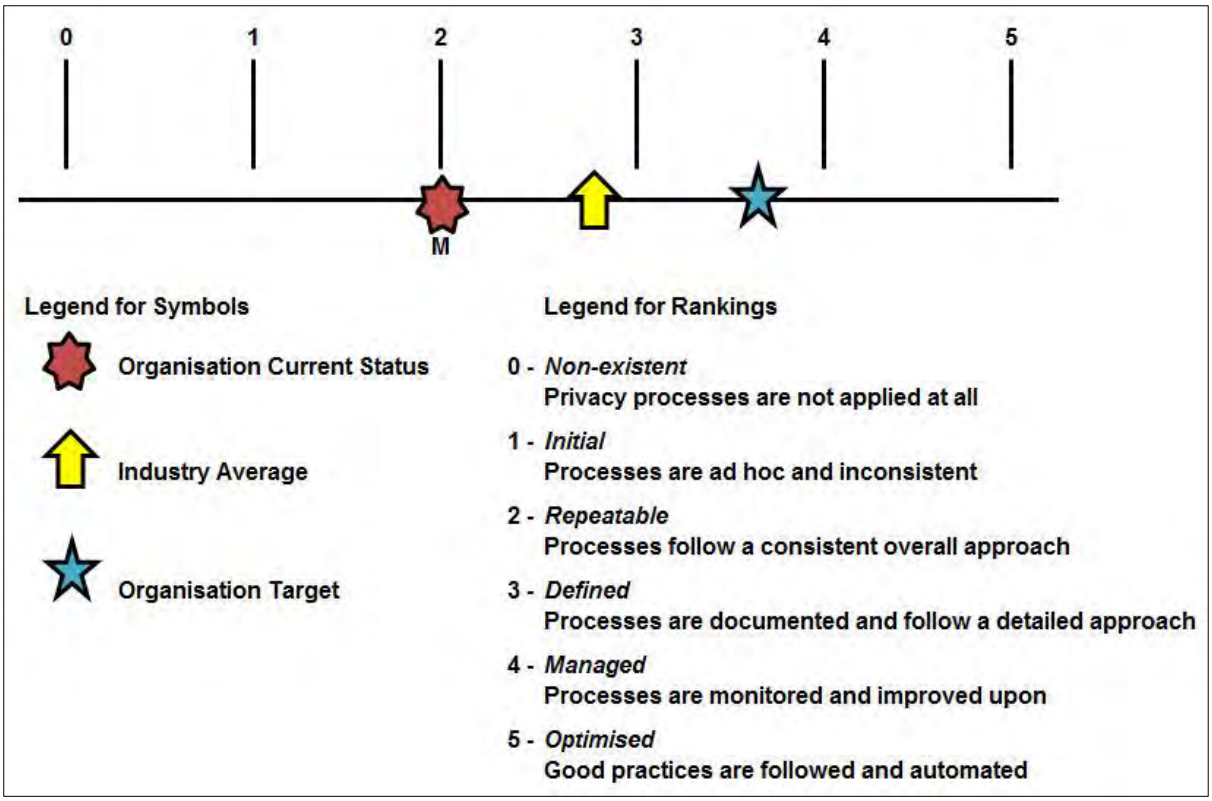

Figure 12: Practical representation of maturity levels

Having calculated the maturity of a Principle an organisation would be able to measure its maturity against an industry average (if this is available) as well as review possible internal maturity targets.

While the PoPI-PMM model provides a calculated level of maturity, it also offers an additional maturity evaluation method based on the policies, processes and business objectives implemented at each of the assessed levels. Utilising both the United States Department of Commerce self-evaluation tool (Office of the CIO, 2006) and the ITIL Maturity Model (Axelos, 2013) a matrix has been developed providing a more practical representation for the business environment. The ITIL Maturity Model provides a list of generic characteristics for each of the CMM maturity levels, while the United States Department of Commerce self-evaluation tool provides seven practical considerations around processes, business objectives and policies. These seven criteria are applied to the generic ITIL characteristics and measured on a scale from *none* to *optimised* (none, ad hoc, consistent, detailed, routine, and optimised). Table 13 provides a view of the “practical” matrix showing the seven criteria, their derived status, and where this places them within the PoPI-PMM maturity levels.

Table 12: Practical business maturity matrix

Privacy Maturity Levels	0 :: Non-existent	1 :: Initial	2 :: Repeatable	3 :: Defined	4:: Managed	5 :: Optimised
Maturity Level Description	*There is no evidence of this standard or practice in the organisation.*	*The organisation has an ad hoc and inconsistent approach to this privacy standard or practice.*	*The organisation has a consistent overall approach, but it is mostly undocumented.*	*The organisation has a documented, detailed approach, but no routine measurement or enforcement of it.*	*The organisation regularly measures its compliance and makes regular process improvements.*	*The organisation has refined its compliance to the level of best practice.*
process consistency	none	ad hoc	consistent	consistent	consistent	consistent
process documentation	none	none	ad hoc	detailed	detailed	detailed
business objectives	none	none	consistent	consistent	optimised	optimised
process measurement	none	none	consistent	routine	optimised	optimised
policy enforcement	none	none	ad hoc	consistent	routine	optimised
process improvement	none	ad hoc	consistent	consistent	routine	optimised
process benchmarking	none	none	none	none	consistent	routine

The inclusion of the practical business maturity matrix is to provide an easier understanding of what the calculated level of maturity represents.

5.4 Construct 3: Protection of Personal Information Act (PoPI)

Incorporating PoPI into the CICA/AICPA privacy maturity model provides for a location specific tool (this process could be adopted for any country where data protection is legislated) which extends global best practice by providing a local solution.

While privacy legislation may vary by geographical location, the CICA/AICPA privacy maturity model remains constant. Each of the ten principles has multiple criteria within it, covering the various elements of privacy best practice (Figure 10, full breakdown in Appendix D). To allow for a granular mapping from the privacy legislation (PoPI in this case) to the privacy maturity model, the legislation is broken down to individual sections and sub-sections. Figure 13 provides a graphical representation of the various sections and sub-sections within PoPI, and Table 13 provides an example of how section 31 of PoPI is broken down into its constituent

parts. While the majority of PoPI sections extend to three levels, there are sections which extend to levels four and five. To provide for the highest level of granularity during the creation of the PoPI-PMM the PoPI Act is broken down to the lowest possible section level.

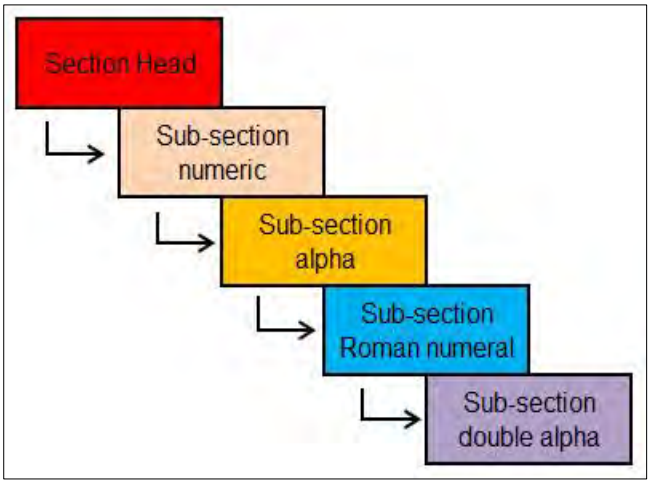

Figure 13: Legislation sectional breakdown

Table 13: PoPI section breakdown

Section Level					
1	2	3	4	5	Full Section
31	1				31(1)
31	1	a			31(1)(a)
31	1	b			31(1)(b)
31	1	b	i		31(1)(b)(i)
31	1	b	ii		31(1)(b)(ii)
31	1	b	ii	aa	31(1)(b)(ii)(aa)
31	1	b	ii	bb	31(1)(b)(ii)(bb)
31	1	b	ii	cc	31(1)(b)(ii)(cc)
31	1	b	iii		31(1)(b)(iii)
31	2				31(2)

Having broken PoPI into its constituent parts it is possible to map the relevant sections to the GAPP framework. However, prior to starting the process it is essential to recognise that a GAPP criterion may allow for multiple PoPI sections to be mapped to it. The manner in which the GAPP criteria are written allows for multiple mappings due to numerous critical key-words used in a single criterion, for example, control 9.2.1 reads:

> **Accuracy and Completeness of Personal Information**
> Personal information is accurate and complete for the purposes for which it is to be used.

This single criterion covers *accuracy*, *completeness* and *purpose,* none of which are represented by a single section within PoPI. Figure 14 outlines the mapping process between individual GAPP criteria and the relevant PoPI sections or sub-sections.

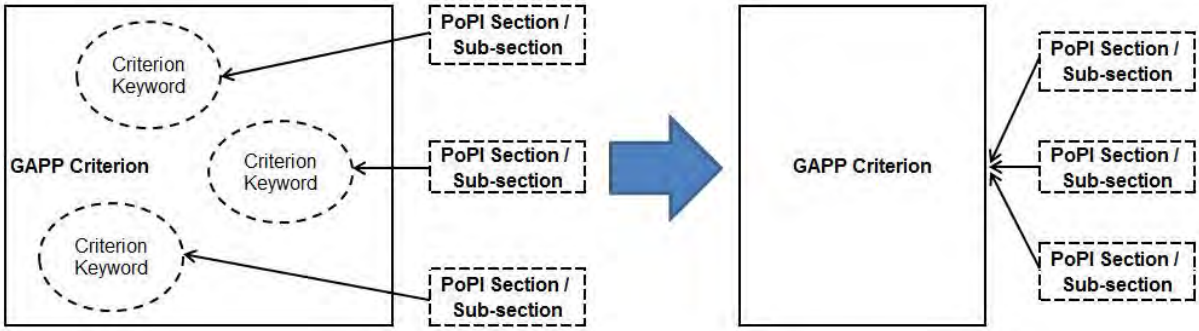

Figure 14: GAPP control keyword mappings

Having separated PoPI into sections and subsections allows for multiple legislative components to be mapped to a single criterion if necessary. Figure 15 provides an outline of the mapping process that is achievable once PoPI has been broken down into its base components.

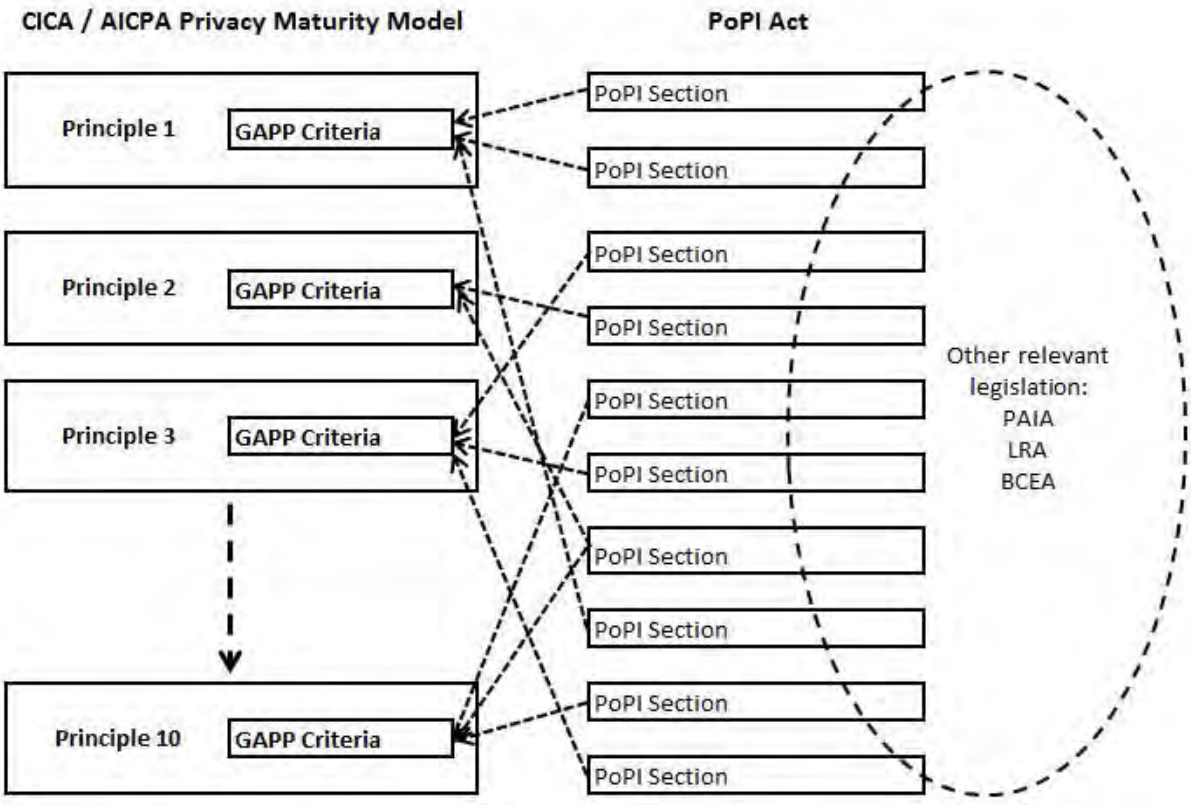

Figure 15: PMM / PoPI mapping process

Although PoPI gives effect to the constitutional right to privacy and sets conditions for how information is processed, there are additional statutes with which organisations need to consider and comply. As mentioned in Chapter 2 these pieces of legislation need to be considered when mapping PoPI to the CICA/AICPA privacy maturity model as they also play a role in the South African corporate landscape.

5.5 Construct 4: Risk

Protecting the privacy of personal information presents organisations with a number of risks to be addressed, including (CICA, 2014):

- Image and Branding – a privacy breach has the potential to impact negatively on an organisation's image, brand and public perception;
- Financial Loss – dependent on an organisation's industry a privacy breach may have direct financial implications (credit card) or indirectly via customer sales or loyalty;
- Shareholder Loss – privacy breaches may impact on shareholders' confidence in an organisation and result in the loss of market capitalisation;
- Regulatory Compliance – failing to comply with regulatory requirements may result in fines and penalties (and negative public perception);
- International Law – not complying with international privacy laws may impact on an organisation's ability to trade with multi-national companies.

The ISO 31000 (2009) / ISO Guide 73:2002 definition of risk is the 'effect of uncertainty on objectives'. In relation to the GAPP framework the following risk matrix could represent the risks associated with the ten principles:

Table 14: Privacy risk matrix (CICA/AICPA, 2013)

No	Privacy Practice	If	Then
1.0	Management	If you do not effectively manage your privacy program,	…your customers will take their business elsewhere.
2.0	Notice	If you do not provide your customer with your privacy notice,	…you may be in violation of PoPI.
3.0	Choice and Consent	If you do not provide your customer with the ability to control when you collect, use and disclose their personal information,	…you may damage customer relations.
4.0	Collections	If you collect more personal information than necessary,	...you may create a greater exposure for abuse of that information.
5.0	Use, Retention and Disposal	If you use the personal information for purposes other than specified,	...you may lose customer trust.
6.0	Access	If you do not give your customers access to their personal information,	...you run the risk of not having accurate customer data.
7.0	Disclosure to Third Parties	If your third-party processor uses the personal information of your customers for purposes other than specified in your contract,	...your customer will still hold you accountable for improper use of that information.
8.0	Security for Privacy	If you do not protect your customer's personal information,	...you run the risk of a significant security breach.
9.0	Quality	If you do not maintain accurate customer data,	…your targeted marketing and sales may suffer.
10.0	Monitoring and Enforcement	If you do not effectively monitor your privacy practices,	...you may be subject to fines and penalties.

While an organisation should undertake a full risk assessment to understand the impact of being non-compliant with privacy legislation (and this would be a recommended procedure), the PoPI-PMM includes a risk weighting option. This is expressed on a 1 (low), 2 (medium), 3 (high) scale, which provides an organisation with a simple framework to identify the risks, rank them in a priority order, and determine what action, if any, must be taken for each based on the estimated cost of the impact. An organisation can identify which, if any, of the ten GAPP Principles carries a higher risk than another. The *risk weighting* (RW) is then used in the calculation of the *weighted maturity ratio* (Wr).

The weighted maturity ratio gives an organisation an indication of privacy maturity incorporating risk. The Wr is calculated as:

$$Wr = \frac{1}{M} RW$$

The reciprocal $(1/x)$ transformation of M is used to achieve a linear correlation between the maturity score (M) and the risk weighting (Wr).The calculated value provides an indication of where an organisation's resources (time, money, and skills) need to be applied based on the measured risk an organisation is willing to accept within its overall capacity – the organisations risk appetite (Barfield, 2007).

5.6 Conceptual Model

Figure 16 illustrates the combined elements of the PoPI-PMM as a conceptual model. Each GAPP criterion has the relevant PoPI sections or subsections mapped to it, and allows for the allocation of a rating between zero and five as per an organisation's maturity level against it. An assessed maturity level can be calculated for each of the ten privacy Principles by calculating the sum of the maturity level for each GAPP criterion and then averaging this by the total number of criteria. In addition to the calculated values depicting the various maturity and weighted maturity levels, an overarching practical maturity measurement is provided by the ITIL maturity framework.

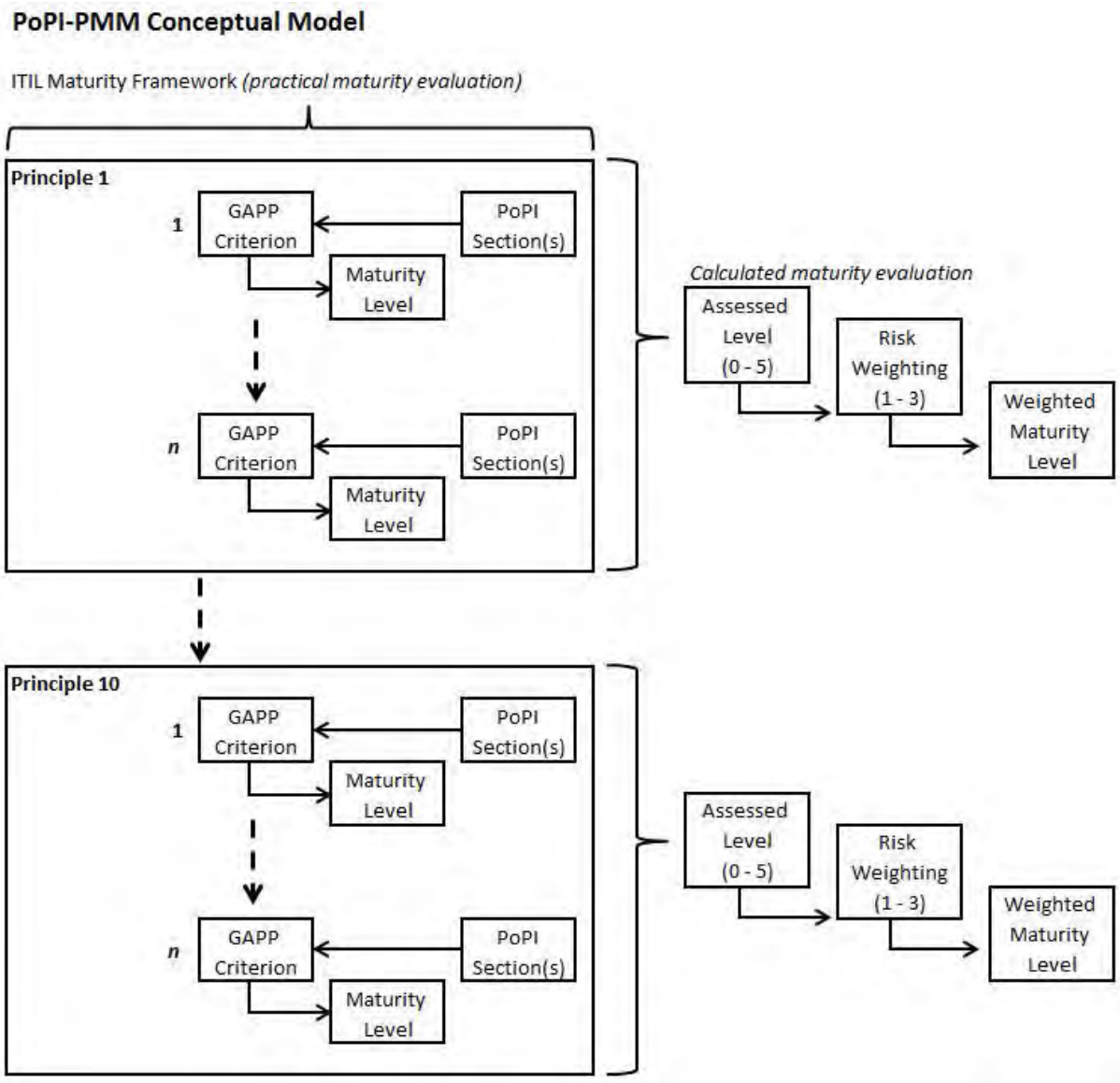

Figure 16: PoPI-PMM conceptual model

5.7 Conclusion

The conceptual model brings together four constructs: 1) the CICA / AICPA GAPP and PMM frameworks; 2) a maturity assessment framework in the form of the CMM; 3) the Protection of Personal Information Act, and finally 4) the ability to assign a risk weighting. As a conceptual model it allows for the interpretation and design of an operational model in multiple formats – paper, database, web-based or mobile. Chapter 6 presents an instantiation of the conceptual model.

6. INSTANTIATION

Having developed the conceptual foundation of the PoPI-PMM this chapter details the instantiation of the model. March and Smith (1995, p. 258) define instantiation as the “realization of an artefact in its environment” and the demonstration of the “feasibility and effectiveness of the models and methods they contain”.

While an instantiation is considered the final output in design science (March & Smith, 1995) there are two research activities identified by March and Smith (1995) that need to be adhered to: build and evaluate. “Build refers to the construction of the artefact, demonstrating that such an artefact can be constructed. Evaluate refers to the development of criteria and the assessment of artefact performance against those criteria” (March & Smith, 1995, p. 258).

This chapter provides the detailed steps in building the artefact – demonstrating its feasibility and answering the question, does it work? The evaluation of the artefact is considered in Chapter 7 – how well does it work, and has progress been made in meeting the research objectives.

6.1 Instantiation Medium

The available development technologies for the PoPI-PMM artefact are numerous – web-based, mobile, database driven, etc. However, due to time constraints and development knowledge, it was decided to utilise Microsoft Excel. The added benefits of using Excel is that it is ubiquitous within the business environment, there is user familiarity with the product, and the artefact can be secured via passwords and locked cells.

The remainder of the chapter will detail the instantiation of the artefact, beginning with privacy maturity levels, practical maturity assessment, the ten Principles and associated criteria, maturity assessment calculations, PoPI mappings, and finally the PoPI-PMM reporting suite which provides organisations with an overview of their maturity levels.

6.2 Privacy Maturity Levels

Having defined the maturity levels as non-existent, initial, repeatable, defined, managed and optimised (refer Figure 11 in Chapter 5); the next step is to provide descriptors for the levels. Table 15 below provides a description for each maturity level which is applied to each of the 73 criteria. The user completing the maturity assessment would select the maturity level most appropriate to the criterion being assessed based on the descriptor for the maturity level.

Table 15: Privacy maturity levels

0 :: Non-existent	1 :: Initial	2 :: Repeatable	3 :: Defined	4:: Managed	5 :: Optimised
There is no evidence of this standard or practice in the organisation.	*The organisation has an ad hoc and inconsistent approach to this privacy standard or practice.*	*The organisation has a consistent overall approach, but it is mostly undocumented.*	*The organisation has a documented, detailed approach, but no routine measurement or enforcement of it.*	*The organisation regularly measures its compliance and makes regular process improvements.*	*The organisation has refined its compliance to the level of best practice.*

6.3 Practical Maturity Assessment

Providing an owner or management team of an organisation with a representation of their maturity based on real-world descriptors concerning their processes, policies and business objectives can provide for a more practical representation than the calculated maturity levels. For this reason, each maturity level corresponds with practical representations of an organisation's maturity in terms of its processes, policies, business objectives, process improvements and benchmarking. This in turn offers a guide to the corresponding level of risk of a privacy breach, or regulatory non-compliance.

Table 16: Privacy risk/regulatory non-compliance

ITIL Characteristics	0 :: Non-existent	1 :: Initial	2 :: Repeatable	3 :: Defined	4:: Managed	5 :: Optimised
process consistency	none	ad hoc	consistent	consistent	consistent	consistent
process documentation	none	none	minimal, high-level	detailed	detailed	detailed
business objectives	not met	not met	partially met	mostly met	fully met	value added
process measurement	none	none	none	ad hoc	routine	optimised
policy enforcement	none	none	none	ad hoc	routine	optimised
process improvement	none	ad hoc	ad hoc	ad hoc	routine	optimised
process benchmarking	none	none	none	ad hoc	ad hoc	routine
Corresponding level of risk of a privacy breach or regulatory non-compliance	***Very high*** *across the organisation*	***High*** *across the organisation, and* ***very high*** *in key parts of the organisation*	***Moderate*** *across the organisation, with some pockets of* ***high*** *risk*	***Moderate*** *across the organisation.*	***Low*** *across the organisation.*	***Remote*** *across the organisation.*

6.4 PoPI-PMM Criteria, Principles and Maturity Calculations

Each of the ten Principles is presented in an expandable group containing the specific criteria associated with that Principle. As a high-level report (Table 17), with all ten Principles viewed in their summary form, an overview of the privacy maturity of an organisation is easily reviewed.

Table 17: PoPI-PMM criteria & principles

PoPI-PMM criteria: / Principles		0 :: Non-existent	1 :: Initial	2 :: Repeatable	3 :: Defined	4:: Managed	5 :: Optimised	Assessed Maturity Level
1.0	Management (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.						1.2
2.0	Notice (5 criteria)	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.						2.4
3.0	Choice and Consent (7 criteria)	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.						2.1
4.0	Collection (7 criteria)	The entity collects personal information only for the purposes identified in the notice.						4.6
5.0	Use, Retention and Disposal (5 criteria)	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.						3.4
6.0	Access (8 criteria)	The entity provides individuals with access to their personal information for review and update.						3.0
7.0	Disclosure to Third Parties (7 criteria)	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.						2.3
8.0	Security for Privacy (9 criteria)	The entity protects personal information against unauthorized access (both physical and logical).						2.3
9.0	Quality (4 criteria)	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.						3.0
10.0	Monitoring and Enforcement (7 criteria)	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.						3.6
								2.8

The Assessed Maturity Level for each Principle is calculated by averaging (the mean) the sum total of all the criteria listed beneath each principle (Table 18). For example, Principle 1 has 14 criteria, with an Assessed Maturity Level of 1.2 which is calculated by adding up all the criteria maturity values (a total of 17 in this example) for Principle 1 and then dividing by the number of criteria, 14 (17/14 = 1.2). The use of the mean, or average, provides for the most “typical” value in a set of values, and

while a concern in using the mean is that the value could be influenced or skewed by outliers, the limited number range available for selection (0 – 5) limits the danger of this.

While the overall privacy maturity of the organisation is represented as an average of the ten Principles, 2.8 in Table 17 above, it is important to emphasize that the Assessed Maturity Level for each principle needs to be viewed independently. The overall privacy maturity level of a business must not distract from any individually immature Principles – all ten Principles require the requisite attention to ensure an organisation is mature.

Table 18 provides an example of the Access Principle in an expanded form where one of the associated criteria (Privacy Principles) is visible. The user marks an "x" in the column which closest describes the entities maturity with that criterion. This process is followed for all 73 criteria provided in the ten Principles. Assigning a value from 0-5 for all 73 criteria provides an Assessed Maturity Level for each of the ten Principles, and an overview of a business's privacy maturity level.

Table 18: Individual criterion

PoPI-PMM criteria: Principles		0 :: Non-existent	1 :: Initial	2 :: Repeatable	3 :: Defined	4:: Managed	5 :: Optimised	Assessed Maturity Level
6.0	ACCESS (8 criteria)	The entity provides individuals with access to their personal information for review and update.						3.0
Privacy Policies (6.1.0)	The entity's privacy policies address the disclosure of personal information to third parties.	No access policies and procedures exist.	Informal disclosure policies and procedures exist but may not be consistently applied.	Disclosure provisions in privacy policies exist but may not cover all aspects, and are not fully documented.	Disclosure provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with disclosure provisions in privacy policies is monitored.	Management monitors compliance with privacy policies and procedures relating to disclosure to third parties. Issues of non-compliance are identified and remedial action taken to ensure compliance.	**2**
				x				

6.4.1 Weighted Maturity Ratio

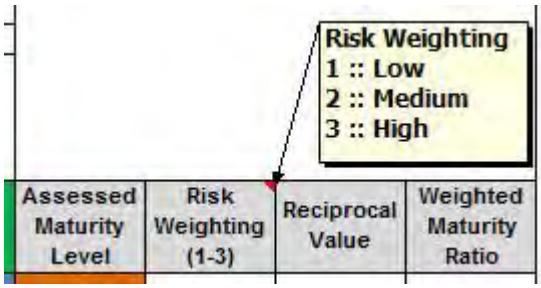

Figure 17: Weighted maturity ratio

The Weighted Maturity Ratio is an additional calculation using a Risk Weighting allocated to a Principle by the organisation. Using a simple three level risk weighting of low (1), medium (2) or high (3) a business is able to identify which Principles are more important within their organisation.

The Weighted Maturity Ratio is calculated by taking the reciprocal value $(1/x)$ of the Assessed Maturity Level multiplied by the risk weighting and multiplied again by a factor of 10 to provide a number that can be represented graphically. Using the reciprocal value of the Assessed Maturity Level allows for a linear correlation between the two variables. While the Assessed Maturity Level provides a rating for the Principles, the Weighted Maturity Ratio attempts to provide a clearer understanding of where an organisation's resources need to be allocated based on the risk associated with the Principle.

Table 19: Weighted maturity ratio workings

PoPI-PMM Principles		Assessed Maturity Level	Risk Weighting	Reciprocal Value	Weighted Maturity Ratio
1.0	Management	**1.2**	1	0.82	8.24
2.0	Notice	**2.4**	1	0.42	4.17
3.0	Choice and Consent	**2.1**	1	0.47	4.67
4.0	Collection	**4.6**	1	0.22	2.19
5.0	Use, Retention and Disposal	**3.4**	1	0.29	2.94
6.0	Access	**3.0**	1	0.33	3.33
7.0	Disclosure to third parties	**2.3**	1	0.44	4.38
8.0	Security for Privacy	**2.3**	2	0.43	8.57
9.0	Quality	**3.0**	1	0.33	3.33
10.0	Monitoring and Enforcement	**3.6**	1	0.28	2.80

As an example (Table 19), Principle 7 and 8 have the same Assessed Maturity Level ratings of 2.3, which if viewed without a risk factor, would indicate that the same amount of resources (time, money, skills) need to be allocated to them to improve their maturity level. However, the organisation has identified Principle 8 as carrying a risk weighting of 2, while Principle 7 is a lesser risk and therefore is allocated 1. The increased risk weighting gives Principle 8 a Weighted Maturity Ratio of 8.57 compared to the 4.38 of Principle 7, implying it requires consideration first. Similarly it can be seen from Table 19 that Principle 1 with a very low maturity level of 1.2, compared to Principle 8's 2.4 would demand priority based on the Assessed Maturity Level. However, employing the Weighted Maturity Ratio, Principle 8 remains the primary concern as it has a Weighted Maturity Ratio of 8.57 compared to 8.24 of Principle 1.

Applying a risk rating to the PoPI-PMM Principles allows the Weighted Maturity Ratio to highlight areas where greater priority should be placed. If a Principle is relatively immature or carries a relatively high risk, it will rate a stronger candidate for organisational resources.

6.5 PoPI Mapping

12	PoPI-PMM Criteria:		Assessed Maturity Level	Risk Weighting (1-3)	Reciprocal Value	Weighted Maturity Ratio
13	Principles					
54	3.0	CHOICE AND CONSENT (7 criteria)	2.1	1	0.47	4.67
55	Privacy Policies (3.1.0)	The entity's privacy policies address the choices to individuals and the consent to be obtained .	2	No relevant section in PoPI		
56						
61	Implicit or Explicit Consent (3.2.1)	Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after The individual's preferences expressed in his or her consent are confirmed and implemented.	3	Section 11(1)(a) Section 11(2)(a) Section 12(2)(b) Section12(2)(c)		
62						
63	Consent for New Purposes and uses (3.2.2)	If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and implicit or explicit consent is obtained prior to such new use or purpose .	2	Section 18(3)		

Figure 18: PoPI mapping

Providing PoPI integration with the maturity assessment tool provides South African businesses with an opportunity to measure their compliance with the new privacy legislation. The relevant PoPI sections have been mapped to the 73 criteria. Where there is no PoPI equivalent the link shows as "No relevant section in PoPI" otherwise the section title is

placed against the criterion – there may be more than one relevant PoPI section per criterion. Within the developed PoPI-PMM spreadsheet the PoPI link clicks through to the full text description of the Act allowing the user to establish the requirements for compliance with the local legislation. The overall effect of the PoPI-PMM is to provide organisations with a sense of their privacy maturity based on a global best practice with the ability to comply with local legislation.

6.6 PoPI-PMM Reports

6.6.1 High-level Overview

The “Results” tab on the PoPI-PMM spreadsheet provides the user with a high-level summary overview of the ten privacy maturity Principles indicating the Principle Maturity Level, Risk Weighting and Weighted Maturity Ratio.

Table 20: PoPI-PMM summary

PoPI-PMM Principles		Assessed Maturity Level	Risk Weighting	Reciprocal Value	Weighted Maturity Ratio
1.0	Management	**1.2**	1	0.82	8.24
2.0	Notice	**2.4**	1	0.42	4.17
3.0	Choice and Consent	**2.1**	1	0.47	4.67
4.0	Collection	**4.6**	1	0.22	2.19
5.0	Use, Retention and Disposal	**3.4**	1	0.29	2.94
6.0	Access	**3.0**	1	0.33	3.33
7.0	Disclosure to third parties	**2.3**	1	0.44	4.38
8.0	Security for Privacy	**2.3**	2	0.43	8.57
9.0	Quality	**3.0**	1	0.33	3.33
10.0	Monitoring and Enforcement	**3.6**	1	0.28	2.80

There are three graphs which provide visual feedback of the corresponding summary in an easy-to-read format which allows for management decisions based on business requirements.

6.6.2 Principle Maturity Spider Graph

The Principle Maturity Level spider graph (Figure 19) is based on the assessed maturity level of each of the ten Principles. The Principles closest to the centre of the graph are the most immature (closest to zero), while the Principles on the outer edge of the graph, closest to five, represent the most mature. Figure 19 provides an initial Principle maturity view with the *Management* Principle being the least mature and therefore closest to the centre of the map, and the *Collection* Principle being the most mature, and therefore on the outer edge of the map.

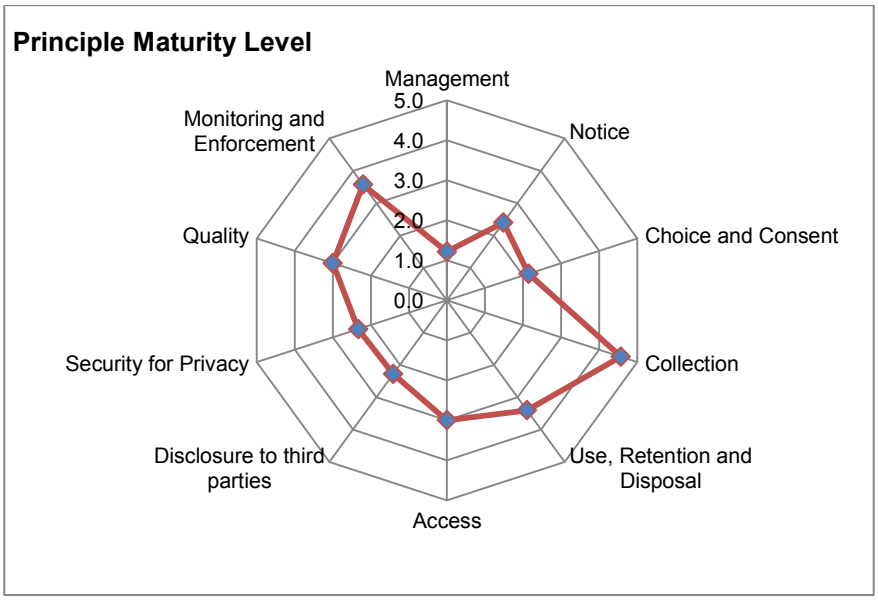

Figure 19: Principle maturity spider graph

6.6.3 Weighted Maturity Ratio Spider Graph

The Weighted Maturity Ratio spider graph (Figure 20) is based on the weighted maturity ratio of the ten Principles. The Principles closest to the centre of the graph require the least attention based on their allocated risk and/or maturity level, while the Principles on the outer edge of the graph represent those requiring immediate attention based on their risk weighting and/or maturity level. While the Principle Maturity Spider Graph identified Principles closest to the centre of the map as requiring attention, the Weighted Maturity Ratio Spider Graph depicts the Principles on the outer edge of the graph as requiring the attention. Figure 20 shows that

Security for Privacy requires priority over *Management* (which is the least mature Principle) due to its higher risk rating allocated by the business.

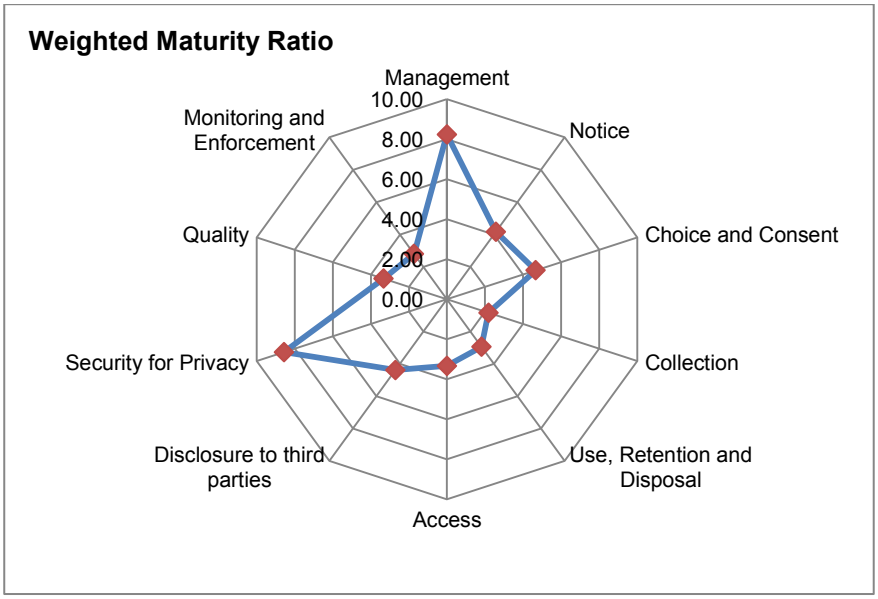

Figure 20: Weighted maturity ratio spider graph

6.6.4 Maturity/Risk Relationship by Principle Graph

The Maturity/Risk Relationship by Principle graph (Figure 21) provides an overview of each Principle's maturity mapped to its associated risk, providing a visual relationship of how the two criteria intersect with one another. The greater the differential between the Principles maturity (blue bar) and risk (striped red bar) will indicate if a Principle requires immediate attention or not. Figure 21 presents the relationship between maturity and risk and indicates that *Management* and *Security for Privacy* require attention, while *Collection* is mature in relation to its risk.

- *Management* and *Security for Privacy*: Each of these Principles' maturity levels is well below their risk rating indicating they require priority attention.
- *Collection*: The maturity level of the Collection Principle far out-weighs the associated risk indicating that the organisation need not invest any more resources in achieving a higher maturity level (it could be argued that resources have been wasted in achieving this maturity level based on the risk to the organisation).

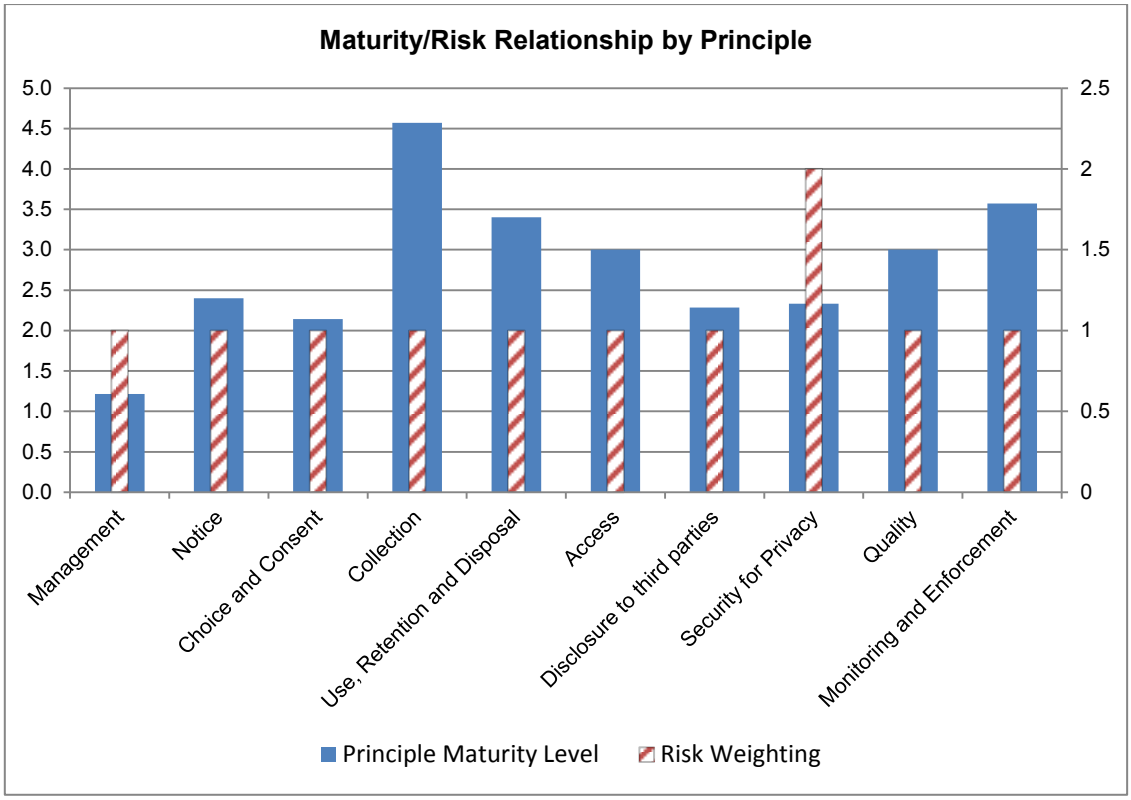

Figure 21: Maturity/risk relationship graph

6.7 Conclusion

The instantiation presented in this chapter shows that the PoPI-PMM model is feasible and can be implemented. While this model focuses on South African privacy legislation there is no reason for it not to be adapted to other geographical locations. Applying the same conceptual development methodology to other privacy legislations will allow for location-specific development.

7. EVALUATION

Having outlined the build process (instantiation) of the PoPI-PMM artefact in Chapter 6, this chapter will evaluate "the development of criteria and the assessment of artefact performance" (March & Smith, 1995, p. 258). Design science consists of iterative cycles (Hevner, 2007; Vaishnavi & Kuechler Jr, 2007), and the development of the PoPI-PMM artefact followed this process. This chapter outlines the development cycles and the evaluation taken within them.

7.1 Design Science Cycles

7.1.1 Cycle 1 – Conceptual Foundation

The literature review conducted for this research indicated that access to current best practice frameworks and standards (Appendix C) would be required, as well as a copy of the Protection of Personal Information Act - No.4 of 2013.

While multiple best practice frameworks and standards were reviewed it was only once the CICA/AICPA privacy maturity model (PMM) and generally accepted privacy principles (GAPP) were reviewed that the foundation for the PoPI-PMM was finalised.

The initial artefact design rested entirely with the researcher. Distilling and mapping the relevant PoPI compliance requirements to the most appropriate GAPP criteria encompassed the first build and evaluate cycle. The initial artefact design lacked rigour as it depended solely on the researcher's knowledge gained over 10 years of working within the field of information security, audit and compliance.

As discussed in Chapter 6, Microsoft Excel was the preferred tool to develop the instantiation. The researcher converted the PoPI Act, GAPP framework and PMM from their native formats into Excel. Once this initial process was complete the researcher was able to map PoPI to the GAPP framework as part of the first build and evaluate cycle.

7.1.2 Cycle 2 – Legal Evaluation

Cycle 2, or the alpha testing phase, required access to a subject matter expert in the field of IT law, governance and audit. Two companies showed interest in assisting with the development of the artefact, however due to various business commitments, only one was able to review the initial artefact.

The researcher had been put in contact with a legal expert (Reviewer A) who currently works within the Information Risk Management (IRM) department of a leading South African financial institution, and asked to remain anonymous. Reviewer A is a qualified attorney providing support from a regulatory/legislative perspective to the IRM team, which is comprised of data protection, information security, data management and records management. Reviewer A is currently involved in a project rolling out the PoPI Act within the financial institution, and works closely with the Act. While Reviewer A works within the IRM department of the financial institution, input was provided in an individual capacity.

Initial correspondence was via email where the researcher outlined the research area and proposed artefact development, and the possibility of a collaborative knowledge sharing process. This was positively received and the first meeting was set-up via Skype due to geographical distance.

The first Skype meeting outlined the requirements for both parties – the researcher needed to provide Reviewer A with the artefact in a certain state of completion, while Reviewer A would review the artefact and provide feedback and queries.

Reviewer A worked on the review process while the researcher continued to build the artefact towards a pilot version. Due to work commitments the initial six-week review period was extended by a further two weeks, after which the artefact was emailed back to the researcher with updates and commentary. A second Skype meeting was set-up.

It was anticipated that this development cycle would constitute multiple iterative reviews providing rigour to the development process. The researcher instituted a change-control and versioning protocol to allow for the iterative process. A second Skype meeting provided specific direction to the development process. Reviewer A

had spent considerable time reviewing the first three PoPI-PMM Principles and had provided commentary and a process of interpreting the PoPI Act. The researcher was required to implement this process for the remaining seven PoPI-PMM Principles prior to returning it for a second review. An additional development presented itself during the review process. While PoPI provided direction for the protection of personal information, and mapped to the GAPP framework well, there were areas where other South African legislation needed to be considered – the Labour Relations Act (1995), Promotion of Access to Information Act (2000) and the Basic Conditions of Employment Act (1997). Reviewer A posed the question as to whether this was to be incorporated in the review process, or if PoPI was to remain the sole reference source. It was decided to incorporate any additional legislation into the process to provide for completeness and ensure all GAPP criteria were addressed.

The researcher implemented the steps suggested by Reviewer A to improve the mapping of PoPI to GAPP, and over a two-week period was able to complete the process and return the artefact for a final review. A further six weeks was required for Reviewer A to review the mapping process and include references to any additional legislation. During this period the researcher continued refining the artefact in preparation for a pilot release with a small to medium enterprise.

On receiving the final reviewed artefact (two reviews within the cycle) the researcher was able to integrate the changes, references, and mappings provided.

7.1.3 Cycle 3 – Organisational Evaluation

Having completed the build and evaluation phase, and having completed a pilot version of the PoPI-PMM framework, there was an opportunity to implement the model. Although the PoPI-PMM framework was only in a pilot stage, design science allows for the instantiation to precede the complete understanding of the underlying model in that it can help show any problematic or incomplete areas within the model.

The implementation phase required access to an organisation, and with an already established relationship with an SME from previous research involving cloud technology adoption (C Hinde & Van Belle, 2012), it was decided to contact the owner (Reviewer B) of ISN (anonymised). Having discussed the pilot project with

Reviewer B, and the possible benefits of participating in the process, there was agreement to participate in the pilot project.

ISN was founded in 1999 and is currently a leading independent provider of outsourced management and administrative services helping organisations align themselves with their business objectives. Consisting of an administration and finance department, sales team, and development and support teams, ISN provided the perfect opportunity to pilot the PoPI-PMM artefact as it maintains both client and employee data, and will be subject to the PoPI Act when a commencement date is announced by the Presidency.

A meeting with Reviewer B was set-up to discuss his availability around using the PoPI-PMM framework, as well as the feedback required to assist with the evaluation process. The importance of the instantiation cycle was to provide the researcher with input on the effectiveness of the artefact in a practical environment and measure its performance.

Reviewer B was able to complete a full evaluation of ISN using the PoPI-PMM framework within two hours. A meeting was set-up to discuss the functionality of the tool and evaluate the results achieved. The PoPI-PMM tool was well received with Reviewer B feeling that “the tool is quite intuitive” and that “it was great in the way it was divided up into the different areas” of information security. While he felt “there are a lot of questions, it’s quite easy, you get to know what the four or five or six different options are, but then the questions become quite tedious.” It was felt the process could be improved if there was a “consultant do it with you”, however “the tool has a lot of potential to go a long way.”

With regards to the results generated by the tool (Table 21), Reviewer B felt it “clearly outlines areas where you are lacking” and that the introduction of PoPI will change the way personal information needs to be considered as “it hasn’t been necessary to track individual’s information in any way in the past”. While ISN scored poorly in the majority of Principles (with a zero maturity level generating an error result of #DIV/0!), Reviewer B felt that “the more knowledge you have about your business, the more you can make decisions moving forward, so the mere fact of knowing where our weaknesses are, now I know how to turn that into a strength”.

Table 21: PoPI-PMM results for ISN

PoPI-PMM Principles		Principle Maturity Level	Risk Weighting	Reciprocal Value	Weighted Maturity Ratio
1.0	Management	0.1	1	7.00	70.00
2.0	Notice	0.0	1	#DIV/0!	#DIV/0!
3.0	Choice and Consent	0.1	1	7.00	70.00
4.0	Collection	0.0	1	#DIV/0!	#DIV/0!
5.0	Use, Retention and Disposal	0.0	1	#DIV/0!	#DIV/0!
6.0	Access	0.6	1	1.60	16.00
7.0	Disclosure to third parties	0.7	1	1.40	14.00
8.0	Security for Privacy	2.6	1	0.39	3.91
9.0	Quality	0.0	1	#DIV/0!	#DIV/0!
10.0	Monitoring and Enforcement	0.6	1	1.75	17.50

In addition to providing a measurable process in defining an organisation's maturity in relation to the PoPI Act, there was the unintentional process of education. While Reviewer B had "read a bit about it" there was no awareness of the impact the Act would have on organisations – "I'm not seeing anything out there that's saying you've got to have this done, even though it's been written into legislation and it is law now." Similar sentiment is expressed in a recent article published in the ITWeb publication iWeek, where Dawie Malan, head of software sales at Ricoh SA, says "most people have a vague notion that PoPI exists and that it concerns the collection of personal information, but the further ramifications escape them" (Pieterse, 2014, p. 21).

While the PoPI-PMM framework constituted a pilot version, the instantiation provided enough evidence that the model was feasible and further development (which was beyond the time frame of this Master's dissertation) would provide a viable business tool.

7.2 Conclusion

The robust build/test/evaluate design science process which guided the development of the PoPI-PMM framework rendered positive results during the instantiation of the pilot artefact. While privacy maturity levels were calculated for the participating SME,

and the owner has been empowered by the results, there was the unexpected benefit of using the framework as an education tool around the PoPI Act. Based on the limited exposure PoPI is receiving in mainstream media, this can be considered beneficial to the overall process.

Due to time constraints of this Master's thesis the successful development of a pilot version of the PoPI-PMM framework (alpha and beta testing) was the extent of this research. While the pilot study rendered favourable results and feedback, additional refinement and further testing with additional organisations would provide generalisation testing.

8. CONCLUSION

This dissertation identified the potential impact the newly enacted Protection of Personal Information Act would have on organisations. While this research only provides initial results, industry research[10] indicates that most organisations (45%) do not have a committee in place to govern PoPI implementation – making this a relevant problem worth addressing. This chapter summarises and reflects on the research contribution and the value of the study.

8.1 Revisiting the Problem Statement

Chapter 1 presented the problem being addressed by this research – the need for a tool to help South African organisations measure their information privacy in relation to the newly enacted PoPI Act (2013). PoPI has the potential to change the business landscape in respect to how organisations collect, use, disclose and store personal information, and the impact could be substantial.

8.2 Meeting the Desired Objectives

The primary objective of this research was the development of a prescriptive model for South African organisations to measure their information privacy maturity in relation to the newly enacted PoPI Act of 2013, which is both easy to use and useful. To address this objective, Chapter 3 established the design science methodology undertaken by this research, while Chapter 4 provided the rationale for developing a privacy maturity model. Chapter 5 developed a detailed conceptual model based on global best practices concerning information security, privacy and risk, as well the privacy legislation that sparked this study. These best practices provided the high-level constructs required to define the model.

In addition to the primary objective, Chapter 1 outlined a number of secondary objectives that would need to be addressed:

- Investigate current best practice frameworks within privacy, information security, personal data protection, data quality, electronic archiving, and risk management.

[10] IT Web PoPI Survey - http://www.itweb.co.za/index.php?option=com_content&view=article&id=134179&Itemid=2894

This dissertation reviewed a number of best practice frameworks within the privacy domain (see Appendix C) before determining that the Generally Accepted Privacy Principles framework developed by the Canadian Institute of Chartered Accountants (CICA) and American Institute of Certified Public Accountants (AICPA) was the best fit.

- Determine the level of compliance required for organisations based on PoPI requirements.
  The first development cycle undertaken by the researcher focused exclusively on utilising the PoPI Act (2013). Engaging with a legal subject matter expert during this first iterative development cycle proved critical in building a robust model. The legal expert extended the requirements of the artefact by including additional legislation which provided an essential element in the finished artefact. This rigorous evaluation ensured that compliance with additional privacy legislation was taken into account.
- Understand the factors that would encourage the use of an artefact within an organisation.
  The instantiation of the artefact provided feedback from the participating organisation. While only a pilot study, the feedback provided constructive input on how to improve and better utilise the artefact should this research be extended. The positive feedback demonstrated the feasibility in continuing with further refinement and generalisation testing.

While the research objectives have been met, the methodology of design science used in this research imposes certain criteria for evaluating projects. The following section explores the design science principles and how this research met those objectives.

8.3 Meeting the Design Science Principles

As discussed in Chapter 3, design science establishes seven requirements for effective research. This section examines the guidelines and how the research satisfies each.

1. *Design as an artefact:* this research produced a number of artefacts including constructs, a model and an instantiation. While the model's foundation was based on an existing framework, the additional constructs provide enough

differentiation to consider it innovative. The inclusion of the PoPI Act (2013) provides for a context-specific artefact.

2. *Problem relevance:* the literature reviewed for this research clearly identified a potential problem. The instantiation of the artefact further confirmed the relevance of the problem at hand.

3. *Design evaluation:* the functionality and usability of the model was confirmed by an instantiation. While this study was limited to a pilot version of the artefact, the inclusion of both legal and organisational input during the development cycles, provided for evidence demonstrating the feasibility of the model as an artefact.

4. *Research contributions:* a novel contribution was made by developing a domain specific model that addresses a new piece of legislation within the South African business environment.

5. *Research rigour:* the model was defined in detail and evaluated both during the design phase by a subject matter expert, as well as the instantiation phase as a pilot study, confirming its real-world veracity.

6. *Design as a search process*: the research process followed a cyclical problem solving process from problem awareness, to suggestion, development and evaluation. The general design-cycle provided for an effective solution.

7. *Communication of research*: Research conducted for this dissertation involved reviewing popular press in relation to the publication of privacy-related articles. The researcher has presented and published conference proceedings (Hinde & Ophoff, 2014) at the 13th annual Information Security South Africa Conference[11] (Appendix E). Furthermore, relevant journals have been identified for publication on completion of the research.

[11] http://www.infosecsa.co.za/

8.4 Research Contributions

The primary driver for this research was the development of a prescriptive model that assisted South African organisations in measuring their existing information privacy maturity – that was achieved. The model adds new knowledge in the field of privacy maturity within a South African context as encapsulated by the PoPI Act. The model uses existing global best practices and standards to provide a solution to the research problem.

While the instantiated model is considered a pilot, the evaluation process provided sufficient evidence to suggest that further refinement (see 8.5 below) could enhance the artefact and allow for generality testing.

The initial review process indicated that PoPI cannot be viewed in insolation of other South African legislation. The legal expert who assisted with the first evaluation cycle of the PoPI-PMM artefact identified additional Act's that needed to be considered in conjunction with PoPI to provide a holistic approach to privacy within South Africa. While PoPI appears self-encapsulating, and a privacy framework can be constructed based on it, the Labour Relations Act (1995), Promotion of Access to Information Act (2000) and the Basic Conditions of Employment Act (1997) need to be considered as well.

An unexpected benefit of this research was the educational aspect. The owner of the organisation who assisted with the evaluation of the PoPI-PMM artefact indicated how the tool added value with regards to exposing him to the PoPI Act. Prior exposure to the Act had been limited, and the impact and requirements of the Act were not fully appreciated. Engaging with the PoPI-PMM artefact provided a better understanding of the PoPI Act and the requirements needed to comply with the legislation.

8.5 Limitations and Recommendations for Future Research

Limitations were introduced by the scope of work and the timelines imposed by the nature of this research. The scope of the artefact was tightly bound with the PoPI Act (2013). Although additional South African legislation is mentioned, it is limited, and extending the artefact to include further legislation that incorporates privacy, labour relations, and legislation restricting access to personal information should be considered.

The calculation of the aggregated maturity level within the artefact follows a very simple formula (summing the value of the criteria within a Principle, and then dividing by the number of criteria). Further research could be conducted to provide for a more exact calculation of the maturity level. In addition, extending the model further with a more refined risk assessment methodology will add value, but this is beyond the scope of the current model.

As mentioned in the contribution section, the one major limitation of this research was the time available to only create a pilot version of the model. Further development will allow for refinement of the model and the opportunity to extend the testing sample to more organisations, therefore providing for a generalised model.

9. APPENDICES

Appendix A – South African Privacy Legislation

The table below provides a summary of current legislation in South Africa that encompasses privacy. Referenced from *Revealing Privacy in South Africa – What you need to know* (Information Security Group of Africa, 2011)

Table 22: Summary of privacy legislation

Legislation	Section	Summary of provision
Constitution of the Republic of South Africa 1996	• Section 14 - Privacy • Section 32 - Access to Information • Section 36 - Limitation of Rights	All Acts within the Republic of South Africa are subject to the Constitution
Promotion of Access to Information Act 2 of 2000	• Section 4 - Records held by official or independent contractor of public or private body • Section 9 - Objects of the Act • Section 63 (1) and (2) - Mandatory Protection of Privacy of Third Party - Natural Person • Section 64 - Mandatory Protection of Commercial Information - Third Party • Section 65 - (Mandatory Protection of Certain Confidential Information - Third Party • Section 66 - Mandatory Protection- Safety of Individuals and Protection of Property • Section 67 - Mandatory Protection - Legally Privileged Records • Section 68 - Commercial information - Private Body • Section 69 - Mandatory Protection - Research Information of Third Party • Section 70 - Mandatory Disclosure - Public Interest • Section 71 - Notice to Third Parties • Section 72 - Representations and Consent - Third Parties • Section 80 - Disclosure of Records to &Non-Disclosure, by Court	The PAIA allows for access to records held by public bodies and information held by the private sector which is required for the exercise or protection of rights.

Electronic Communications and Transactions Act 25 of 2002	• Section 50 - Protection of Personal Information: Scope of Protection of Personal Information • Section 51 - Principles for Electronic Collection of Personal Information • Section 86 - Unauthorised Access, Interception, Interface with Data	Regulates electronic transactions, digital signatures, authentication and cryptography, privacy and data protection, consumer protection in the online environment, and the liability of infrastructure and connectivity providers for third party content that is transmitted over their systems.
National Credit Act, Act 34 of 2005	• Part A – Interpretation • Part B - Confidentiality, personal information and consumer credit records (Section 67 - Conflicting Legislation) • Part B - Confidentiality, personal information and consumer credit records Section 68 - Right - Confidential Treatment	To promote a fair and non-discriminatory marketplace for access to consumer credit and for that purpose to provide for the general regulation of consumer credit and improved standards of consumer information.
Consumer Protection Act 68 of 2008	• Section 11 - Consumer's Right – Privacy; Right to restrict unwanted direct marketing • Section 107 - Offences and Penalties; Breach of Confidence	The CPA applies to the promotion of goods and services that could lead to certain transactions, as well as to most transactions occurring within South Africa for the supply of goods and services concluded in the ordinary course of business between suppliers and consumers.
Regulation of Interception of Communications Act 70 of 2002	• Section 2: Prohibition - Interception of Communication • Section 3: Interception of Communication under Interception Direction • Section 4: Interception of Communication by Party to Communication • Section 5: Prior Written Consent • Section 6: Interception of Indirect Communication - Connection with carrying on of business	To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information.

Appendix B – South African Corporate Legislation

Summary of legislation covering businesses in South Africa:

Table 23: Business legislation summary for South Africa (ENS,(2013))

Legislation	Summary of provision
Constitution of the Republic of South Africa 1996	All Acts within the Republic of South Africa are subject to the Constitution
Companies Act 71 of 2008	To provide for the incorporation, registration, organisation and management of companies, the capitalisation of profit companies, and the registration of offices of foreign companies carrying on business within the Republic; to define the relationships between companies and their respective shareholders or members and directors; to provide for equitable and efficient amalgamations, mergers and takeovers of companies; to provide for efficient rescue of financially distressed companies; to provide appropriate legal redress for investors and third parties with respect to companies.
Auditing Profession Act 26 of 2005	To provide for the education, training and professional development of registered auditors; to provide for the accreditation of professional bodies; to provide for the registration of auditors; to regulate the conduct of registered auditors.
Labour Relations Act 66 of 1995	To regulate the organisational rights of trade unions; to promote and facilitate collective bargaining at the workplace and at sectoral level; to regulate the right to strike and the recourse to lock-out in conformity with the Constitution; to promote employee participation in decision-making through the establishment of workplace forums.
Promotion of Access to Information Act 2 of 2000	The PAIA allows for access to records held by public bodies and information held by the private sector which is required for the exercise or protection of rights.
Promotion of Administrative Justice Act 3 of 2000	To give effect to the right to administrative action that is lawful, reasonable and procedurally fair and to the right to written reasons for administrative action as contemplated in section 33 of the Constitution of the Republic of South Africa.
Public Finance Management Act 1 of 1999	To regulate financial management in the national government and provincial governments; to ensure that all revenue, expenditure, assets and liabilities of those governments are managed efficiently and effectively; to provide for the responsibilities of persons entrusted with financial management in those governments.
Securities Services Act36 of 2004	Regulates securities services and is aimed at increasing confidence in the South African financial markets, promoting the protection of regulated persons and clients, reducing systemic risk and promoting the international competitiveness of securities in South Africa.
Banks Act94 of 1990	To provide for the regulation and supervision of the business of public companies taking deposits from the public, and to provide for matters connected therewith.
The Income Tax Act 58 of 1962	To consolidate the law relating to the taxation of incomes and donations, to provide for the recovery of taxes on persons, to provide for the deduction by employers of amounts from the remuneration of employees in respect of certain tax liabilities of employees, and to provide for the making of provisional tax payments and for the payment into the National Revenue Fund of portions of the normal tax and interest and other charges in respect of such taxes, and to provide for related matters.

Customs and Excise Act 91 of 1964	To provide for the levying of customs and excise duties and a surcharge; for a fuel levy, for a Road Accident Fund levy, for an air passenger tax and an environmental levy; the prohibition and control of the importation, export, manufacture or use of certain goods; and for matters incidental thereto.
The Securities Transfer Tax Act 25 of 2007	Provides for the levying of a securities transfer tax in respect of every transfer of any security on or after 1 July 2008.
Broad-Based Black Economic Empowerment Act 53 of 2003	BEE is a prominent government policy and socio-economic process which seeks to contribute to the economic transformation of South Africa by bringing about significant increases in the number of black people that manage, own and control the country's economy, and by bringing about significant decreases in income inequalities.
Financial Advisory and Intermediary Services Act 37 of 2002	FAIS provides for the regulation of certain financial advisory and intermediary services and, in addition to establishing the Office of Ombud for Financial Services Providers, has established codes of conduct for financial service providers in South Africa.
Financial Intelligence Centre Act 38 of 2001	FICA brings South Africa in line with international efforts to curb money-laundering and the financing of terrorist activities.
Financial Intelligence Centre Amendment Act 11 of 2008	FICA was amended by the Financial Intelligence Centre Amendment Act 11 of 2008 on 1 December 2010.
Prevention of Organised Crime Act 121 of 1998	POCA has introduced various and significant measures to assist in the combating of organised crime in South Africa.
Competition Act 89 of 1998	The overarching aim of the Competition Act is to ensure effective, fair and vigorous competition in the market.
Competition Amendment Act 1 of 2009	The Amendment Act is not intended to overhaul the current competition law regime. Instead it strengthens the Act around anti-competitive practices, collusive tendering and market division and a more proactive role in investigating markets & take measures to ensure market transparency.
Consumer Protection Act 68 of 2009	The CPA applies to the promotion of goods and services that could lead to certain transactions, as well as to most transactions occurring within South Africa for the supply of goods and services concluded in the ordinary course of business between suppliers and consumers.
National Credit Act 34 of 2005	To promote a fair and non-discriminatory marketplace for access to consumer credit and for that purpose to provide for the general regulation of consumer credit and improved standards of consumer information.
Short Term Insurance Act 53 of 1998	To provide for the registration of short-term insurers; for the control of certain activities of short-term insurers and intermediaries.
Long Term Insurance Act 52 of 1998	To provide for the registration of long-term insurers; for the control of certain activities of long-term insurers and intermediaries.
Labour Relations Act 66 of 1995	This governs protections for employees against unfair dismissal and unfair labour practices in employment, and regulates the resolution of disputes between employers and employees, as well as strikes, lockouts and the relationship between employers and trade unions.
Basic Conditions of Employment Act 75 of 1997	To give effect to the right to fair labour practices referred to in section 23(1) of the Constitution by establishing and making provision for the regulation of basic conditions of employment; and thereby to comply with the obligations of the Republic as a member state of the International Labour Organisation.
Occupational Health and Safety Act 85 of 1993	The employer has a general duty to provide and maintain a working environment that is safe, and without risk to employees' health.
Compensation for Occupational Injuries and Diseases Act 130 of 1993	To provide for compensation for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment, or for death resulting from such injuries or diseases.

Employment Equity Act 55 of 1998	The EEA prohibits unfair discrimination (direct or indirect) in any employment policy or practice.
National Environmental Management Act 107 of 1998	Environmental legislation that aims to protect the environment while pursuing sustainable economic growth on terms applicable to a developing nation.
National Water Act 36 of 1998	The primary legislation governing the use and pollution of fresh water.
National Environmental Management: Waste Act 59 of 2008	Provides for national norms and standards for the storage, collection, transportation, treatment, disposal, re-use and recycling of waste in general as well as hazardous waste.
Hazardous Substances Act 15 of 1973	To provide for the control of substances which may cause injury or ill-health to or death of human beings by reason of their toxic, corrosive, irritant, strongly sensitising or flammable nature or the generation of pressure thereby in certain circumstances, and for the control of certain electronic products.
The Mineral And Petroleum Resources Development Act 28 of 2002	The state exercises sovereignty over all the mineral resources within the Republic of South Africa.
Electronic Communications and Transactions Act 25 of 2002	Regulates electronic transactions, digital signatures, authentication and cryptography, privacy and data protection, consumer protection in the online environment, and the liability of infrastructure and connectivity providers for third party content that is transmitted over their systems.
The Films and Publications Act 65 of 1996	To provide for the classification of certain films and publications; to that end to provide for the establishment of a Film and Publication Board and a Film and Publication Review Board.
The National Gambling Amendment Act 10 of 2008	Entrenches the legality of engaging in online gambling, but seeks to regulate the e-gambling industry more tightly.
Electronic Communications Act 36 of 2005	To promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors and to provide the legal framework for convergence of these sectors; to make new provision for the regulation of electronic communications services, electronic communications network services and broadcasting services.
Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002	Electronic communications networks and systems may be intercepted and monitored under South African law.
The Trade Marks Act 194 of 1993	To provide for the registration of trademarks, certification trademarks and collective trademarks
The Copyright Act 98 of 1978	Provides statutory protection of copyright in South Africa.
Patents Act 57 of 1978	Patent protection may be obtained for inventions which are new and non-obvious, and which are capable of use in the fields of trade, industry or agriculture.

Appendix C – Best Practice Standards and Frameworks

Table of standards and frameworks that were considered for this research:

Table 24: Standards and frameworks

International Organization for Standardization (ISO Standards)	
ISO8000	Standard for data quality
ISO9000	Quality management systems
ISO14641	Electronic archiving
ISO27000	Information security management systems
ISO29100	Security techniques - Privacy framework
ISO29101	Security techniques - Privacy reference architecture
ISO31000	Risk management

COBIT (Information Systems Audit and Control Association - ISACA)
Framework for IT management and governance; links business / IT goals; provides metrics and maturity models; identifies responsibilities of business & IT process owners

Information Technology Infrastructure Library (ITIL)
A set of practices for IT service management; aligns IT services with business needs; processes, procedures, tasks and checklists for establishing integration with the business's strategy.

American Institute of CPAs	
GAPP	Generally Accepted Privacy Principles Framework

European Committee for Standardisation	
CWA 15499-2	Personal Data Protection Audit Framework (EU Directive EC 95/46)

British Standards (BSi)	
British Standard– BS10012:2009	Personal Information Management System

Appendix D – GAPP Framework

Table 25: GAPP framework (CICA/AICPA, 2009)

Generally Accepted Privacy Principles and Criteria (GAPP Framework)					
1.0	Management	1.1	Policies and Communications	1.1.0	Privacy Policies
				1.1.1	Communication to Internal Personnel
				1.1.2	Responsibility and Accountability for Policies
		1.2	Procedures and Controls	1.2.1	Review and Approval
				1.2.2	Consistency of Privacy Policies and Procedures with Laws and Regulations
				1.2.3	Personal Information Identification and Classification
				1.2.4	Risk Assessment
				1.2.5	Consistency of Commitments With Privacy Policies and Procedures
				1.2.6	Infrastructure and Systems Management
				1.2.7	Privacy Incident and Breach Management
				1.2.8	Supporting Resources
				1.2.9	Qualifications of Internal Personnel
				1.2.10	Privacy Awareness and Training
				1.2.11	Changes in Regulatory and Business Requirements
2.0	Notice	2.1	Policies and Communications	2.1.0	Privacy Policies
				2.1.1	Communication to Individuals
		2.2	Procedures and Controls	2.2.1	Provision of Notice
				2.2.2	Entities and Activities Covered
				2.2.3	Clear and Conspicuous
3.0	Choice and Consent	3.1	Policies and Communications	3.1.0	Privacy Policies
				3.1.1	Communication to Individuals
				3.1.2	Consequences of Denying or Withdrawing Consent
		3.2	Procedures and Controls	3.2.1	Implicit or Explicit Consent
				3.2.2	Consent for New Purposes and Uses
				3.2.3	Explicit Consent for Sensitive Information
				3.2.4	Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices
4.0	Collection	4.1	Policies and Communications	4.1.0	Privacy Policies
				4.1.1	Communication to Individuals
				4.1.2	Types of Personal Information Collected and Methods of Collection

		4.2	Procedures and Controls	4.2.1	Collection Limited to Identified Purpose The collection of personal information is limited to that necessary for the purposes identified in the notice.
				4.2.2	Collection by Fair and Lawful Means
				4.2.3	Collection From Third Parties
				4.2.4	Information Developed about Individuals
5.0	Use, Retention, and Disposal	5.1	Policies and Communications	5.1.0	Privacy Policies
				5.1.1	Communication to Individuals
		5.2	Procedures and Controls	5.2.1	Use of Personal Information
				5.2.2	Retention of Personal Information
				5.2.3	Disposal, Destruction and Redaction of Personal Information
6.0	Access	6.1	Policies and Communications	6.1.0	Privacy Policies
				6.1.1	Communication to Individuals
		6.2	Procedures and Controls	6.2.1	Access by Individuals to Their Personal Information
				6.2.2	Confirmation of an Individual's Identity
				6.2.3	Understandable Personal Information, Time Frame, and Cost
				6.2.4	Denial of Access
				6.2.5	Updating or Correcting Personal Information
				6.2.6	Statement of Disagreement
7.0	Disclosure to Third Parties	7.1	Policies and Communications	7.1.0	Privacy Policies
				7.1.1	Communication to Individuals
				7.1.2	Communication to Third Parties
		7.2	Procedures and Controls	7.2.1	Disclosure of Personal Information
				7.2.2	Protection of Personal Information
				7.2.3	New Purposes and Uses
				7.2.4	Misuse of Personal Information by a Third Party
8.0	Security for Privacy	8.1	Policies and Communications	8.1.0	Privacy Policies
				8.1.1	Communication to Individuals
		8.2	Procedures and Controls	8.2.1	Information Security Program
				8.2.2	Logical Access Controls
				8.2.3	Physical Access Controls
				8.2.4	Environmental Safeguards
				8.2.5	Transmitted Personal Information
				8.2.6	Personal Information on Portable Media
				8.2.7	Testing Security Safeguards

9.0	Quality	9.1	Policies and Communications	9.1.0	Privacy Policies
				9.1.1	Communication to Individuals
		9.2	Procedures and Controls	9.2.1	Accuracy and Completeness of Personal Information
				9.2.2	Relevance of Personal Information
10.0	Monitoring and Enforcement	10.1	Policies and Communications	10.1.0	Privacy Policies
				10.1.1	Communication to Individuals
		10.2	Procedures and Controls	10.2.1	Inquiry, Complaint, and Dispute Process
				10.2.2	Dispute Resolution and Recourse
				10.2.3	Compliance Review
				10.2.4	Instances of Noncompliance
				10.2.5	Ongoing Monitoring

Appendix E – ISSA Conference Publication

BIBLIOGRAPHY

Abor, J., & Quartey, P. (2010). Issues in SME Development in Ghana and South Africa. *International Research Journal of Finance and Economics*, (39), 218–228.

Ahern, D. M., Clouse, A., & Turner, R. (2004). *CMMI distilled: a practical introduction to integrated process improvement* (2nd ed.). Addison-Wesley Professional.

AICPA/CICA. (2011). AICPA/CICA Privacy Maturity Model User Guide. AICPA/CICA. Retrieved from http://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf

Aluchna, M. (2009a). Does good corporate governance matter? Best practice in Poland. *Management Research News*, *32*(2), 185–198.

Aluchna, M. (2009b). Implementation of best practice code: practical implications from the Warsaw Stock Exchange. *Social Responsibility Journal*, *5*(1), 123–140.

Axelos. (2013, October). ITIL Maturity Model. Axelos Limited. Retrieved from https://www.axelos.com/gempdf/ITIL_Maturity_Model_v1_2W.pdf

Banisar, D., & Davies, S. (1999). Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *John Marshall Journal of Computer & Information Law*, *18*(1), 1–108.

Barfield, R. (2007). Risk appetite—How Hungry are You? *The Journal: Special Risk Management Edition*, 8–13.

Baskerville, R. (2008). What design science is not. *European Journal of Information Systems*, *17*(5), 441–443.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering*, *1*(3), 213–222.

Benbasat, I., Dexter, A. S., Drury, D. H., & Goldstein, R. C. (1984). A critque of the stage hypothesis: theory and empirical evidence. *Communications of the ACM*, *27*(5), 476–485.

Boswell, W. R., Bingham, J. B., & Colvin, A. J. (2006). Aligning employees through "line of sight." *Business Horizons*, *49*(6), 499–509.

Cambridge Advanced Learner's Dictionary & Thesaurus. (2013). research noun - definition in the British English Dictionary & Thesaurus - Cambridge Dictionaries Online. Retrieved June 25, 2014, from http://dictionary.cambridge.org/dictionary/british/research_1?q=research

Camp, R. C. (1989). *Benchmarking: the search for industry best practices that lead to superior performance*. Milwaukee: Quality Press.

Cannon, D. L. (2011). *CISA Certified Information Systems Auditor Study Guide*. Hoboken, NJ: John Wiley & Sons.

Chan, Y. E., & Greenaway, K. E. (2005). Theoretical explanations for firms' information privacy behaviors. *Journal of the Association for Information Systems*, *6*(6), 7.

CICA. (2014). Privacy resources - frequently asked questions | Chartered Accountants of Canada. Retrieved July 17, 2014, from http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/faqs/item10442.aspx#Whatisprivacy-relatedrisk

CICA/AICPA. (2009, August). Generally Accepted Privacy Principles. CICA/AICPA. Retrieved from

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf

Clarke, R. (1997). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Retrieved July 7, 2013, from http://www.rogerclarke.com/DV/Intro.html

Collins, J., & Hussey, R. (2003). *Business Research: a practical guide for undergraduate and postgraduate students*. New York: Palgrave Macmillan.

Cornish, J. (2013). South Africa's Protection of Personal Information Bill: The Law of Unintended Consequences? Latham and Watkins. Retrieved from http://www.lw.com/presentations/POPI-The-Law-of-Unintended-Consequences

Cowles, M. G. (2001). Who writes the Rules of E-Commerce. *A Case Study of the Global Business Dialogue on E-Commerce (GBDe). Washington, DC: American Institute of Contemporary German Studies*.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003.

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). Understanding the main phases of developing a maturity assessment model. Presented at the Australasian Conference on Information Systems (ACIS), Sydney.

Deloitte. (2014, March 17). POPI Compliance. Retrieved from http://deloitteblog.co.za/tag/popi-compliance/

Dennedy, M. F., Fox, J., & Finneran, T. (2014). *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. Apress. Retrieved from http://books.google.co.za/books?id=3_cFAwAAQBAJ

ENSafrica. (2013). *General corporate information for foreign clients: establishing a business in South Africa* (p. 75). ENS. Retrieved from http://mandarin.ensafrica.com/Doing%20Business%20in%20SA.pdf

Fisher, D. (2004, September). The Business Process Maturity Model: A Practical Approach for Identifying Opportunities for Optimization. Bearing Point. Retrieved from http://www.bptrends.com/bpt/wp-content/publicationfiles/10-04%20ART%20BP%20Maturity%20Model%20-%20Fisher.pdf

Fraser, P., Moultrie, J., & Gregory, M. (2002). The use of maturity models/grids as a tool in assessing product development capability (Vol. 1, pp. 244–249). Presented at the Engineering Management Conference, 2002. IEMC'02. 2002 IEEE International, IEEE.

Fromholz, J. M. (2000). European Union Data Privacy Directive, The. *Berk. Tech. LJ*, *15*, 461.

Gagnon, M. A., Jansen, K. J., & Michael, J. H. (2008). Employee alignment with strategic change: A study of strategy-supportive behavior among blue-collar employees. *Journal of Managerial Issues*, *XX Number 4*(Winter 2008), 425–443.

Galup, S., Quan, J. J., Dattero, R., & Conger, S. (2007). Information technology service management: an emerging area for academic research and pedagogical development. In *Proceedings of the 2007 ACM SIGMIS CPR conference on Computer personnel research: The global information technology workforce* (pp. 46–52). ACM.

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly*, *26*(1), 75–81.

Grant Thornton. (2014, March 6). SA businesses are not ready for new privacy protection legislation. Retrieved August 4, 2014, from http://www.gt.co.za/news/2014/03/sa-businesses-are-not-ready-for-new-privacy-protection-legislation-grant-thornton/

Gray, D. E. (2009). *Doing research in the real world*. Sage.

Greenaway, K., & Chan, Y. (2013). Designing a Customer Information Privacy Program Aligned with Organizational Priorities. *MIS Quarterly Executive*, *12*(3).

Greenberg, A. (2013). The Data Breach Blog. Retrieved from http://www.scmagazine.com/the-data-breach-blog/section/1263/

Gregg, D. G., Kulkarni, U. R., & Vinzé, A. S. (2001). Understanding the philosophical underpinnings of software engineering research in information systems. *Information Systems Frontiers*, *3*(2), 169–183.

Hakes, C., Popplewell, B., Gallacher, H., & Clements, G. (1995). *The corporate self assessment handbook: for measuring business excellence* (3rd ed.). Chapman & Hall New York.

Hammer, M. (2007). The process audit. *Harvard Business Review*, *85*(4), 111.

Harden, S. (2007, October). Fill the GAPP. Retrieved May 29, 2014, from http://www.calcpa.org/Content/24730.aspx

Harmon, P. (2004, March). Evaluating an Organization's Business Process Maturity. Retrieved from http://www.simprocess.net/pdf/BPtrendLevelEval1to5.pdf

Harrop, N., Gillies, A., & Wood-Harper, A. (2012). "Actors" and "clients": why systems dynamics needs help from soft systems methodology and

unbounded systems thinking. *Journal of the Operational Research Society*, *63*(12), 1788–1789.

Harty, N. (2013, January). New Privacy Laws - Preparing for PoPI. Newsletter. Retrieved from http://www.harty.co.za/ServeFile.cfm?FileID=88

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, *19*(2), 4.

Hiebeler, R., Kelly, T., & Ketteman, C. (2012). *Best practices: Building your business with customer-focused solutions*. Simon and Schuster.

Hinde, C., & Ophoff, J. (2014). Privacy: A Review of Publication Trends (pp. 1 – 7). Presented at the Information Security South Africa, Johannesburg. Retrieved from http://icsa.cs.up.ac.za/issa/2014/Proceedings/Full/64_Paper.pdf

Hinde, C., & Van Belle, J. (2012). Cloud Computing in South African SMMEs: Risks and Rewards for Playing at Altitude. *International Journal of Computer Science and Electrical Engineering*, *1*(1), 1–10.

Holvast, J., Madsen, W., & Roth, P. A. (1999). *The Global Encyclopaedia of Data Protection Regulations*. Kluwer Law International. Retrieved from http://books.google.co.za/books?id=TsvQkQEACAAJ

Hughes, D., & Smart, P. (1994). The development and testing of a computer based tool to assist strategy formulation. In *IEE Conference Publications* (pp. 312–317). IET.

Hurley, D., & Mayer-Schönberger, V. (2000). Information policy and governance. *Governance in a Globalizing World*.

Information Security Group of Africa. (2011). *Revealing privacy in South Africa: What you need to know*. Information Security Group of Africa.

International Organization for Standardization. (2009). ISO 31000: 2009 Risk management–Principles and Guidelines. *International Organization for Standardization, Geneva, Switzerland*.

IT Governance Institute. (2014). ITGI. Retrieved July 2, 2014, from http://www.itgi.org/

Kim, S. (2006). *Safeguarding Consumer Privacy in a Technological Era: A Comparison of Privacy Protections in New Zealand and California*. Fulbright New Zealand Fellowship Office.

King, J. L., & Kraemer, K. L. (1984). Evolution and organizational information systems: an assessment of Nolan's stage model. *Communications of the ACM*, *27*(5), 466–475.

Kobrin, S. J. (2004). Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, *30*(1), 111–131.

Kulkarni, U., & Freeze, R. (2004). Development and validation of a knowledge management capability assessment model (p. 14). Presented at the International Conference on Information Systems (ICIS).

Lamprecht, I. (2013, June 3). Few organisations ready for Popi. Retrieved August 4, 2014, from http://www.moneyweb.co.za/moneyweb-south-africa/few-organisations-ready-for-popi

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2009). Developing maturity grids for assessing organisational capabilities: Practitioner guidance. Presented at the

4th International Conference on Management Consulting, Academy of Management (MCD), Vienna, Austria.

Manson, N. (2006). Is operations research really research? *ORiON: The Journal of ORSSA*, *22*(2), 155–180.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of research design and methodology.* John Wiley & Sons Inc.

Marsoof, A. (2008). The right to privacy in the information era: A south Asian perspective. *SCRIPT-Ed*, *5*(3), 1–22. doi:10.2966/scrip.050308.553

Matthes, C. (2014, February 19). Unpacking the POPI Act: | iWeek Magazine. Retrieved August 9, 2014, from http://www.iweek.co.za/on-the-cover/unpacking-the-popi-act

McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (Technical Report No. SP 800-122) (pp. 1–59). Gaithersburg, MD, United States: National Institute of Standards & Technology.

McCormack, K., Willems, J., Van den Bergh, J., Deschoolmeester, D., Willaert, P., Štemberger, M. I., … Vuksic, V. B. (2009). A global investigation of key turning points in business process maturity. *Business Process Management Journal*, *15*(5), 792–815.

Mettler, T., & Rohner, P. (2009). Situational maturity models as instrumental artifacts for organizational design. In *Proceedings of the 4th international conference on design science research in information systems and technology* (p. 22). ACM.

Michalson, L. (2009, August 24). Protection of Personal Information Bill – the implications for you. Retrieved March 13, 2014, from http://www.michalsons.co.za/protection-of-personal-information-bill-the-implications-for-you/3041

Michalsons. (2011, March 31). The Consumer Protection Act – a heads up. Retrieved April 12, 2014, from http://www.michalsons.co.za/the-consumer-protection-act-a-heads-up/1382

Mingers, J. (1997). Multi-paradigm Methodology. In Mingers and Gill (Ed.), *Multimethodology*. Chichester: John wiley and Sons.

Moody, D. L., & Shanks, G. G. (1994). What Makes a Good Data Model? Evaluating the Quality of Entity Relationship Models. In *Entity-Relationship Approach-ER'94. Business Modelling and Re-Engineering: 13th International Conference on the Entity-Relationship Approach, Manchester, United Kingdom, December 13-16, 1994 Proceedings* (Vol. 881, p. 94). Springer.

Movius, L. B., & Krup, N. (2009). US and EU privacy policy: Comparison of regulatory approaches. *International Journal of Communication*, *3*, 19.

Myers, M. D., & Venable, J. R. (2014). A set of ethical principles for design science research in information systems. *Information & Management*.

Neethling, J., Potgieter, J. M., & Visser, P. J. (1996). *Neethling's law of personality*. Durban: Butterworths.

Office of the CIO. (2006, March 24). Data Security Maturity Model. Retrieved from https://ocio.osu.edu/assets/IT-Security/ITsec-matureselfasses.xls

Ooi, K.-B., & Darmawan, N. (2011). Does employee alignment affect business-IT alignment? An empirical analysis. *Journal of Computer Information Systems*, (Spring 2011), 10–20.

Oxford Dictionary. (2014). Oxford Dictionaries. Retrieved August 9, 2014, from http://www.oxforddictionaries.com/

Park, L. (2014, February 26). Data Breach Trends. Retrieved August 4, 2014, from http://www.symantec.com/connect/blogs/data-breach-trends

Paulk, M., Curtis, B., Chrissis, M. B., & Weber, C. (1993). *Capability Maturity Model for Software, Version 1.1* (Techincal No. CMU/SEI-93-TR-024) (p. 82). Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalReport/1993_005_001_16211.pdf

Pearson, S. (2012). Privacy Management in Global Organisations. In B. De Decker & D. Chadwick (Eds.), *Communications and Multimedia Security* (Vol. 7394, pp. 217–237). Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-642-32805-3_23

Peterson, D., Meinert, D., Criswell II, J., & Crossland, M. (2007). Consumer trust: privacy policies and third-party seals. *Journal of Small Business and Enterprise Development*, *14*(4), 654–669.

Pieterse, I. (2014, June). SMEs lack POPI awareness. *iWeek Magazine*, (June 2014), 21–23.

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. Presented at the European Conference on Information Systems (ECIS), Frankfurt.

Price Waterhouse Coopers. (2011). *The Protection of Personal Information Bill: The Journey to Implementation* (p. 38). South Africa: Price Waterhouse Coopers.

Retrieved from http://www.pwc.co.za/en_ZA/za/assets/pdf/popi-white-paper-2011.pdf

Privacy Rights Clearing House. (2013). Chronology of Data Breaches: Security Breaches 2005 - Present. Retrieved June 22, 2014, from http://www.privacyrights.org/data-breach

Protection of Personal Information Act, No.4 of 2013. Protection of Personal Information Act, Pub. L. No. No. 4 of 2013 (2013). Retrieved from www.gov.za/documents/download.php?f=204368

Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169.

Rummler, G. A., & Brache, A. P. (2012). *Improving performance: How to manage the white space on the organization chart*. John Wiley & Sons.

Scheppele, K. L. (1988). *Legal Secrets: Equality and Efficiency in the Common Law*. University of Chicago Press. Retrieved from http://books.google.co.za/books?id=XE46te6SxHgC

Schroeder, D. (2011, July). GAPP Targets Privacy Risks. Retrieved May 29, 2014, from http://www.journalofaccountancy.com/Issues/2011/Jul/20103191.htm

Scott, J. E. (2007). Mobility, business process management, software sourcing, and maturity model trends: propositions for the IS organization of the future. *Information Systems Management*, *24*(2), 139–145.

Simon, H. (1996). *The sciences of the artificial* (3rd ed.). Cambridge, MA: MIT Press.

Simonsson, M., Johnson, P., & Wijkström, H. (2007). Model-based IT governance maturity assessments with COBIT. Presented at the In Proceedings of the European Conference on Information Systems (ECIS), St. Gallen, Switzerland.

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

South Africa Law Reform Commission. (2005, October 13). Media Statement by the SALRC on its investigation into privacy and data protection (project 124). Retrieved from http://www.justice.gov.za/salrc/media/2005-prj_124_media.pdf

Spanyi, A. (2004, July). Towards Process Competence. Business Process Management Group. Retrieved from http://www.spanyi.com/images/BPM%20Towards.pdf

Teo, T. S., & King, W. R. (1997). Integration between business planning and information systems planning: an evolutionary-contingency perspective. *Journal of Management Information Systems*, 185–214.

University of Miami. (2014). What is personally identifiable information? Retrieved May 29, 2014, from http://privacyoffice.med.miami.edu/faq/privacy-faqs/what-is-personally-identifiable-information-pii

Vaishnavi, V. K., & Kuechler Jr, W. (2007). *Design science research methods and patterns: innovating information and communication technology*. CRC Press.

Vaishnavi, V., & Kuechler, B. (2004). Design Research in Information Systems. Retrieved February 9, 2014, from http://www.desrist.org/design-research-in-information-systems/

Volio, F. (1981). Legal personality, privacy and the family. In L. Henkin (Ed.), *The International Bill of Rights: The Covenant on Civil and Political Rights*. Columbia University Press. Retrieved from http://books.google.co.za/books?id=1QJZSAAACAAJ

Von Baum, F. (2012, February 2). New draft European data protection regime also to apply to all US compa- nies processing data of European residents. m law

group. Retrieved from http://www.mlawgroup.de/news/publications/pdf/2012_02_01-EU_data_protection.pdf

Weber, C., Curtis, B., & Gardiner, T. (2008, June). Documents Associated With Business Process Maturity Model (BPMM), Version 1.0. Object Management Group. Retrieved from http://www.omg.org/spec/BPMM/1.0/PDF/

White House. (1997). A framework for global electronic commerce. *Washington: White House*.

Zysman, J., & Weber, S. (2001). Governance and Politics of the Internet Economy–Historical Transformation or Ordinary Politics with a New Vocabulary? *Berkeley Roundtable on the International Economy*.

Privacy: A Review of Publication Trends

Charlie Hinde* and Jacques Ophoff†
Centre for Information Technology and National Development in Africa (CITANDA)
Dept. of Information Systems
University of Cape Town
Cape Town, South Africa
Email: *charliehinde@gmail.com †jacques.ophoff@uct.ac.za

***Abstract*—The huge growth in digital data and the commercialisation of personal information has brought privacy to the forefront of world legislation. The impact and growth of the Internet, digitisation of data, network connectivity and data sharing has required a number of new threats to be addressed. As the technological environment has expanded since the 1960's and the use of electronic commerce has become more ubiquitous, so the concern around privacy and personal information protection has increased. Privacy is important at various levels and allows people to develop their individuality apart from the groups to which they belong and offers them the ability to decide what face they want others to see. Based on the recent Snowden leaks there is currently a heightened interest in privacy and related issues worldwide.**

The IEEE Security & Privacy magazine is one of the leading publications devoted to privacy, providing articles with both a practical and research focus by leading thinkers within the security and privacy field. The magazine has a broad audience which includes practitioners, researchers and policy-makers. The objective of this paper is to provide a systematic review of how privacy has been reported in the magazine over the past decade. The paper examines the shifts of privacy within the information security domain, with particular interest to the past three years which have seen revisions and amendments in various national privacy policies. In addition to reviewing the magazine there is input from the magazine's current editor, who shares her views and insights on both the magazine and privacy in general.

Findings show that over the period 2011–2013, privacy articles were predominantly driven by academic research, with the majority of security articles coming from within industry. There is little evidence that privacy has become a more dominant topic over the past ten years. While data loss and security breaches have escalated over the past decade the topic of privacy has taken second place to security.

***Index Terms*—Privacy, Managing Information Security.**

I. Introduction

The rise in information security breaches over the past five years, through either malicious intent or systems weakness, has shown how vulnerable our personal information is to abuse. The theft of laptops, loss of unencrypted USB drives, hackers infiltrating servers, staff deliberately accessing client's personal information, etc. are all regularly reported [1], [2].

The huge growth in digital data and the commercialisation of personal information has brought privacy to the forefront of South African, and world, legislation. The impact and growth of the Internet, digitisation of data, network connectivity and data sharing has required a number of new threats to be addressed. In South Africa, the Protection of Personal Information (PoPI) Act is an attempt to address privacy and lists a number of privacy commitments that businesses will need to attend to: transparency in the form of clear communications with clients; respect of people's personal information; a data subjects choice of whether their personal information can be shared; the accountability of users of personal data; and ensuring that privacy design is part of any new initiative, product or service and complies with regulatory requirements.

Despite this regulation it is not clear how much importance the topic of privacy receives, either from a personal or an informational perspective. Is privacy important in today's society and are there recurring debates? This high-level systematic review of the IEEE Security & Privacy magazine highlights the reporting of privacy-related articles over the magazine's ten year history. The review initially highlights all privacy-related articles before focussing on the past three years (2011–2013) in an attempt to see if there is a reporting trend that correlates to security breaches.

The overall objective of this paper is to provide a high-level review of how privacy has been reported over the past decade. The huge growth in digital data and the commercialisation of personal information has brought privacy to the forefront of world legislation. The impact and growth of the Internet, digitisation of data, network connectivity and data sharing has required a number of new threats to be addressed. This paper seeks to review the shifts, if any, of privacy within the information security domain, with particular interest to the past three years which have seen revisions and amendments in various national privacy policies.

The paper proceeds as follows: first several perspectives on privacy is given through a literature review. Next the research methodology and reviewed articles are discussed. The data analysis and a discussion of the results follows, before the paper is concluded.

II. Literature Review

Data privacy and data security are often used interchangeably. Data security is defined as the preservation of confidentiality, integrity and availability of data [3], or the practices and processes that are put in place to ensure data is being accessed by the right people. Data privacy is concerned with the appropriate use of data – is data used according to the agreed purposes at the time of collection [4].

A. What is Privacy – An Overview

The Oxford Dictionary defines privacy, as "the state of being left alone and not watched or disturbed by other people". A person's right to privacy is extended further than being merely 'left alone' and includes the right to having control over his or her personal information and the ability to conduct their personal affairs relatively free from unwanted intrusions [5]. Considered a fundamental human right it is recognised by the Universal Declaration of Human Rights , the International Covenant on Civil and Political Rights and in many other international and regional treaties [6]. Although privacy has deep seated roots in history (the law of privacy can be traced as far back as 1361, when the English Justices of the Peace Act provided for the arrest of peeping toms and eavesdroppers [6]), it is considered one of the most difficult human rights to define. While the definition of privacy describes how far society can intrude into a person's affairs, privacy advocates describe privacy as having several aspects or categories [6]–[8]:

- Information privacy, involving the establishment of rules governing the collection and handling of personal data such as credit information and medical records
- Bodily privacy, concerning the protection of people's physical beings against invasive procedures such as drug testing and cavity searches
- Privacy of communications, covering the security and privacy of mail, telephones, email and other forms of communication
- Territorial/physical privacy, concerning the setting of limits on intrusion into the domestic and other environments such as the work place or public space

B. Privacy and Data Protection

As the technological environment has expanded since the 1960's, and the use of electronic commerce has become more ubiquitous, so the concern around privacy and personal information protection has increased [9], [10]. The advent of electronic communication has removed the obstacles of distance and time when transferring information and with this has come the possibility of information or data being intercepted and falling into the hands of unintended parties [8].

As the digitisation of information continues into the foreseeable future the question of whether privacy is distinct from data protection needs to be answered. The Information Technology Act of India, section 2(o), provides a comprehensive definition of data:

> ...data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

Using this definition, data protection indicates the protection of information that can be generated using computer systems. Utilising the definition of data and applying it to the categories (aspects) of information privacy and privacy of communications mentioned earlier, it becomes apparent that data protection is also an aspect of privacy.

C. Why is Information Privacy Important?

As the sophistication of information technology escalates, and the interconnectivity of networks providing unprecedented methods of collecting, analysing and disseminating information on individuals increases, so the concern of the invasion of privacy, or the potential of invasion, increases correspondingly. [6] extend the technological aspects of privacy invasion to include three important trends:

- Globalisation removes geographical limitations to the flow of data - the development of the Internet is perhaps the best known example of a global technology
- Convergence is leading to the elimination of technological barriers between systems. Modem information systems are increasingly inter-operable with other systems, and can mutually exchange and process different forms of data
- Multi-media fuses many forms of transmission and expression of data and images so that information gathered in a certain form canbe easily translated into other forms

[11] provides four reasons why privacy is important, and these become more evident when considering the ease of proliferation of information, and the corresponding invasion thereof:

- Privacy is psychologically important: "People need private space. . . . We need to be able to glance around, judge whether the people in the vicinity are a threat, and then perform actions that are potentially embarrassing."
- Privacy is sociologically important: "People need to be free to behave and to associate with others, subject to broad social mores, but without the continual threat of being observed."
- Privacy is economically important: "People need to be free to innovate. International competition is fierce, so countries with high labour-costs need to be clever if they want to sustain their standard-of-living. And cleverness has to be continually reinvented."
- Privacy is politically important: "People need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and threatens democracy."

Privacy allows people to develop their individuality apart from the groups to which they belong and offers them the ability to decide what face they want others to see [12].

D. The Costs of Protecting Privacy

While the protection of privacy outlined by [11] offers benefits to both society and individuals it must be tempered with the associated costs. While privacy allows individuals the opportunity to decide "what face they want others to

see it is not an absolute good because it imposes real costs on society" [12, p. 465]. A broadly defined privacy right allows for the opportunity of withholding true information from society therefore protecting some individual rights at the expense of others. Promoting the possibility of misinformation can have both social and economic impacts as people are less able to make fully informed decisions such as whether a "child's babysitter had been convicted for child abuse or whether a physician had a history of malpractice" [12, p. 465].

The midpoint between too little or too much privacy is what progressive governments need to find the balance between. When looking at global privacy legislation there tends to be a minimum level of privacy protection without a maximum set [12]. In the case of South African legislation "the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests" [4].

E. International Privacy Legislation

Apart from the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, internationally privacy has been recognised as an important right to be protected. The advent of globalisation and economic imperatives has brought with it the need for nations to cooperate at numerous levels, one of which is ensuring the privacy of individuals.

The genesis of modern privacy legislation can be traced back to the Land of Hesse in Germany in 1970 which then prompted countries like Sweden (1973), Germany (1977) and France (1977) to follow suit [6]. Using this early legislation as a foundation two crucial international instruments evolved – The Council of Europe's (COE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data , and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. Both instruments lay out specific rules covering the handling of electronic data which now forms the core of many global data protection laws [6].

The European Union has extended the COEs 1981 legislation to take into consideration the globalisation of the information economy [13] and currently utilises the 1995 Data Protection Directive (in January 2012 the European Commission unveiled a draft European General Data Protection Legislation which will supersede the Data Protection Directive [14]). While Europe has legislated data privacy at a national level the United States has followed an industry-based self-regulation process. This laissez-faire governance system, where markets set the industry agenda, has resulted in existing legislation that is reactive and issue-specific [15], and is characterised as a "patchwork quilt" [16, p. 1] with no single overarching privacy law [17].

Globally there are many countries that now protect privacy under human rights legislation within their Constitutions: Kingdom of the Netherlands (Constitution of the Kingdom of the Netherlands, 1989), Republic of the Philippines (Part III, Constitution of the Republic of the Philippines, 1987), and the Russian Federation (art 23, Constitution of the Russian Federation, 1993). While the definition of data protection may vary across international laws and declarations, the attributes of personal information are consistently described as being: obtained fairly and lawfully; used only for the original specified purpose; adequate, relevant and not excessive to purpose; accurate and up to date; accessible to the subject; kept secure; and destroyed after its purpose is completed [6].

F. South African Privacy Legislation

In South Africa the right to privacy is protected in terms of both common law and the in the Constitution (section 14). However, the right to privacy is not absolute and consideration is given to competing interests such as maintaining law and order, protecting commercial interests, and the administration of national social programs [18]. While the right to privacy is balanced with other rights entrenched in the Constitution the recognition it has within the Constitution as a fundamental human right indicates its importance.

Apart from the Constitution (and common law) there is currently no legislation which deals specifically and fully with information protection [18]. In November 2000 the South African Minister of Justice and Constitutional Development requested the South African Law Reform Commission (SALRC) to investigate concerns around the protection of personal information. In September 2003 the SALRC published a comprehensive Issue Paper for information and comment entitled "Privacy and Data Protection" (known as Project 124) and received written comment from 34 persons and institutions. In October 2005 the SALRC published a Discussion Paper with draft legislation and invited comment towards the creation of the PoPI Bill (B9-2009).

In May 2009 the SALRC approved the investigation into privacy and data protection that the Minister of Justice initiated in 2000. The subsequent PoPI Act will protect individuals' personal information by penalising organisations and other parties that do not adequately protect personal information [13]. The objective of PoPI is to regulate the processing of personal information by public and private bodies while working within international standards – particularly European legislation.

Having outlined the concepts and challenges of privacy, the next section discusses the research methodology, including the rationale for the sample chosen.

III. Research Methodology

In order to gain an insight into digital privacy developments a descriptive literature review was undertaken. The review retrospectively analysed a decade's worth of privacy-related articles. The articles analysed was limited to the IEEE Security & Privacy magazine (S&P). S&P consists of an annual volume with six issues published and was first published in January 2003. The magazine currently has an impact factor of 0.9 [19].

S&P is one of 160 journals, magazines and research collections published by the IEEE. Providing articles with both a practical and research focus by leading thinkers within the

TABLE I
KEYWORD SEARCH LIST

Keyword Search Terms	No. of Articles
Privacy (information)	88
Security (information)	22
Data (protected/sharing)	14
Information Security (personal)	14
Identity (management)	9
Assurance (policy)	7
Law (privacy)	4
Personal information (data)	4
Policies (privacy)	4
Regulation (privacy)	2
Total	168

security and privacy field, the magazine provides case studies, tutorials, columns, book reviews, and in-depth interviews from within the information security industry.

The objective of S&P is best quoted as per their website [1]:

> The primary objective of IEEE Security & Privacy is to stimulate and track advances in information assurance and security and present these advances in a form that can be useful to a broad cross-section of the professional community-ranging from academic researchers to industry practitioners. It is intended to serve a broad readership.

S&P is envisioned to provide a unique combination of research articles, case studies, tutorials, and regular departments covering diverse aspects of information assurance such as legal and ethical issues, privacy concerns, tools to help secure information, analysis of vulnerabilities and attacks, trends and new developments, pedagogical and curricular issues in educating the next generation of security professionals, secure operating systems and applications, security issues in wireless networks, design and test strategies for secure and survivable systems, and cryptology [1].

According to the editor S&P opted to publish as a magazine (and not a journal) because "we have a broad audience: practitioners, researchers and policy-makers, and we try to make our articles accessible to all three types of readers. So, unlike a journal, which tends to report research by and for researchers, we try to inform our readers in an accessible way about the things they need to do their jobs" [20].

Having identified S&P as a reputable source of information, the indexes of each publication were captured into Microsoft Excel from the IEEE Xplore Digital Library. Each magazine index was then grouped per year and converted to a tabular format for easier analysis. Having obtained all the indexes and grouping them by their respective years, a keyword search was applied according to the words, or groupings of words, found in the titles of the articles to differentiate possible privacy-related articles. The results are shown in Table I in decreasing order of frequency. Note that an article could contain multiple keywords.

Applying the keywords, and reviewing the context in which they were used in the title of the article, provided an initial base for the identification of articles pertaining to privacy. A high-level abstract review of each article then followed to ensure no mismatches occurred. The initial application of the keywords provided a high correlation to the overall article-count and only three mismatched articles were identified following the abstract review and removed.

Having identified mismatched articles the data was then checked for any magazine volumes that revealed no privacy-related articles. The sub-categories of Privacy Interests and S&P Economics were subsequently reviewed for possible missing articles. This second review process provided an additional five articles which were initially missed by the keyword search as the respective terms were not in the article title. These articles were subsequently added to the overall total of privacy-related articles.

The next section presents the publication trends of privacy-related articles. It also presents possible explanations for these trends.

IV. DATA ANALYSIS AND DISCUSSION

The total number of privacy-related articles was 133. The distribution of privacy-related articles over a ten year period is illustrated in Table II. The first seven years show a fairly consistent publication of privacy-related articles. However, consideration needs to be given to the fact that the magazine prints on average approximately 100 articles per year, of which privacy articles make-up on average 13 articles of the total per annum (13%). In addition, the magazine offers insight into relevant topics in each issue by providing a "special edition" focusing on a central theme. There was no indication that these special editions included an additional focus on privacy-related topics.

The article count indicated a shift from the lowest recorded number of privacy-related articles (7) to the highest number (16) over the ten year period (see Figure 1), which could indicate a shift in public perception of privacy, or possibly legislative changes. With this in mind each privacy-related article from 2011-2013 was reviewed and summarised to provide insight into the increased article count over the three year period.

A. Privacy vs. Practice in 2011

There is a marked drop in privacy-related articles in 2011, as shown in Table III. Compared to 2010, half as many privacy articles appear in 2011, with the 4th volume of 2011 not having a single article. The predominant feature throughout the year's publications revolved around security, cyber-attacks, encryption, and secure IT infrastructure. This correlated closely to what was happening in the "IT world" in general, as a review of 2011 revealed major concerns around:

- hacktivism
- malicious code being spread by social media and the web (the Stuxnet worm was still a hot topic although it had been uncovered in 2010)
- attacks on high profile businesses like RSA

TABLE II
PRIVACY-RELATED ARTICLES BY YEAR

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	Total
Issue 1	2	3	3	2	2	2	3	2	2	2	2	25
Issue 2	4	3	2	1	1	4	2	1	2	1	2	23
Issue 3	1	1	1	3	3	1	2	1	1	1	8	23
Issue 4	1	2	1	2	1	1	3	4	0	1	2	18
Issue 5	2	1	2	1	4	5	1	1	1	2	2	22
Issue 6	4	3	1	3	2	1	1	5	1	1	0	22
Total	14	13	10	12	13	14	12	14	7	8	16	133

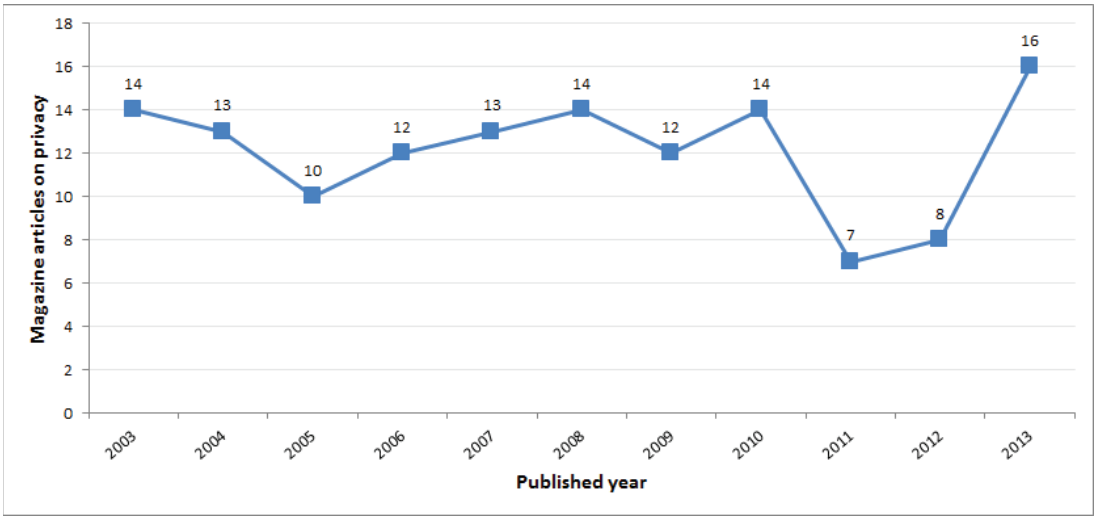

Fig. 1. Privacy-related Articles Published in S&P

- the undermining of SSL certificates and the companies that provide them (Comodo, GlobalSign, Digicert, OpenSSL and DigiNotar)
- the increase of bring your own device (BYOD) within business and the rise of the smartphone and the mobile revolution
- cyber warfare and the targeting of national assets, e.g. electricity grids [21], [22]

B. Privacy vs. Practice in 2012

Data from 2012 (illustrated in Table IV) reveal a similar pattern to 2011 with most of the focus on authentication, security, infrastructure security, software security, cyber warfare and cryptography. The magazine continued to run special editions throughout the year looking mainly at security related issues. Reviewing two security focused websites, Security Week and Sophos, 2012 is deemed to be another year where security lagged behind hackers and social engineering in terms of data breaches. Web servers and databases remained easy targets with IT professionals not implementing security policies and procedures effectively. Cybercriminal toolkits continued to evolve, mostly in response to security anti-virus firms understanding the shifts in security requirements. The growth of smartphones in 2012, with continued integration with social media platforms, improved technologies like near field communication (NFC) and GPS becoming pervasive in applications, provided greater exploitation mechanisms for both security and privacy [23], [24].

C. Privacy vs. Practice in 2013

The sudden increase in privacy-related articles in 2013 (illustrated in Table V) seems to be a direct response to the increase in online social networks activity, combined with the huge growth in smartphones and the BYOD phenomenon that IT departments throughout business are grappling with. The third volume of S&P in 2013 is dedicated to “Privacy & Online Social Networks” with 6 direct articles and 2 indirect articles – the largest single publication looking at privacy making up almost 50% of the articles for the volume. However, it must be noted that if the special edition focusing on privacy did not appear in 2013, the article count would be similar to the previous two years, with only 10 articles appearing after 5 volumes (volume 6 had not been published at the time of this review).

Reviewing the European Union Agency for Network and Information Security (ENISA) 2013 mid-year report shows a continued upward trend in malware, SQL code injections, exploit kits, botnets, identity theft and the abuse of information leakage [25]. While securing networks, servers, databases and websites requires IT security solutions like encryption, secure certification, password management and user authentication, the continued breaches that occur across all business sectors [2] indicates that utilising a technology-only approach is limited.

TABLE III
ARTICLES IN 2011

Issue	Includes Special Edition	Special Edition Topic	Special Edition Articles	Privacy-related Articles
1	Yes	Engineering Secure Systems	3	2
2	Yes	Shouldn't All Security Be Usable?	2	2
3	Yes	The Science of Security	3	1
4	No	–	–	0
5	Yes	Cyber warfare	4	1
6	Yes	Living with Insecurity	6	1

TABLE IV
ARTICLES IN 2012

Issue	Includes Special Edition	Special Edition Topic	Special Edition Articles	Privacy-related Articles
1	Yes	Authentication – Are We Doing Well Enough?	4	2
2	Yes	Security Training and Education	4	1
3	Yes	Software Assurance for the Masses	4	1
4	Yes	Internet Infrastructure Security	5	1
5	Yes	E-voting Security	5	2
6	Yes	Lost Treasures	5	1

TABLE V
ARTICLES IN 2013

Issue	Includes Special Edition	Special Edition Topic	Special Edition Articles	Privacy-related Articles
1	Yes	A View from the C-Suite	4	2
2	Yes	Transferring Security Technology	4	2
3	Yes	Privacy & Online Social Networks	6	8
4	Yes	Safety-Critical Systems	3	2
5	No	–	–	2
6	N/A	Not published at time of writing	–	–

TABLE VI
PRIVACY-RELATED ARTICLES BY SOURCE

Year	Academic	Non-Academic	Mixed	Total
2011	6	1	0	7
2012	5	2	1	8
2013	9	5	2	16
Total	20	8	3	31

D. Discussion

Reviewing the privacy-related articles from 2011–2013 provides an interesting observation – the majority of articles are written from an academic perspective (see Table VI). This is despite the fact that S&P is not a traditional academic journal.

From an academic perspective, a method of influencing privacy is by approaching government or regulatory bodies. In the United States the Federal Trade Commission (FTC), which comprises the Bureaus of Competition, Economics, and Consumer Protection, is the only federal agency with general jurisdiction over unfair and deceptive privacy practices. According to [26, p. 79] "the FTC's work is greatly facilitated by input from academic research communities, journalists, and independent researchers." [26, p. 82] continues by saying that research within the privacy field often aims to "directly inform technically sound policy decisions for everyone from national governments to end users."

It is interesting to note that over the period 2011–2013 privacy articles were predominantly driven by academic research, with the majority of security articles coming from within industry. According to the S&P editor the biggest shift with respect to privacy is:

> ...the robust discussion based on Snowden's (Edward Snowden, the former NSA contractor who leaked US government surveillance secrets) recent revelations; before that, many people were ready to say that there is no longer any such thing as privacy. Now, that said, I'd say the European privacy directive laid the groundwork for the Snowden-related discussions.

The interplay between academia, industry and regulators is an important factor and should be taken into account in any intended publication to ensure that it is well-rounded.

V. CONCLUSION

The high-level systematic analysis of privacy-related articles within S&P provided little evidence that privacy has become a more dominant topic over the past ten years. While data loss and security breaches have escalated over the past decade the topic of privacy has taken second place to security.

No matter the strength of the preventative methods, guidelines or processes put in place, people continue to unwittingly hand over personal information (including passwords and other credentials). While social engineering has become sophisticated there is still a trusting naivete among users. The continued technological escalation between fraudster and IT security at times neglects the end user, and it is evident that technology on its own does not provide the only solution towards stopping privacy breaches. This is echoed by the editor of S&P, who notes that the biggest shifts in privacy noted over

the years is that “a lot of technologists thought that technology would solve privacy problems; now I think they are realizing that it takes a combination of technology and policy – so the conversation is more informed by behavioural scientists than it used to be” [20]. The recent revelations published by Edward Snowden of the mass surveillance programs conducted by the United States, Israeli and British governments will hopefully shift the reporting of privacy from sporadic articles, to a more front-and-centre status as the public realize that privacy is a human right still worth protecting.

A limitation of this research is it’s focus on a single publication for review. Future research can build on it’s findings by adding additional journals or conference proceedings (academic as well as industry conferences such as Black Hat or DefCon) to affirm the identified trends. Investigation into reports of security breaches and privacy leaks can also provide additional insight into the academic versus professional reactions to these events.

REFERENCES

[1] Security & Privacy, IEEE, “Security & privacy, IEEE,” 2013. [Online]. Available: http://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=8013

[2] Privacy Rights Clearinghouse, “Public policy & reports,” 2013. [Online]. Available: https://www.privacyrights.org/speeches-testimony

[3] ISO/IEC, “ISO 27001: Information technology - security techniques - information security management systems - requirements,” 2005.

[4] Minister of Justice and Constitutional Development, “The protection of personal information bill,” 2012.

[5] J. Neethling, J. Potgieter, and P. Visser, *Neethling’s law of personality*. Butterworths, 1996. [Online]. Available: http://books.google.co.za/books?id=c2c_AQAAIAAJ

[6] D. Banisar and S. Davies, “Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments,” *John Marshall Journal of Computer & Information Law*, vol. 18, no. 1, pp. 1–108, 1999.

[7] S. Kim, “Safeguarding consumer privacy in a technological era: A comparison of privacy protections in new zealand and california,” Fulbright New Zealand, Tech. Rep., 2006. [Online]. Available: http://www.fulbright.org.nz/wp-content/uploads/2011/12/axford2006_kim.pdf

[8] A. Marsoof, “The right to privacy in the information era: A south asian perspective,” *SCRIPT-ed*, vol. 5, no. 3, 2008.

[9] D. Hurley and V. Mayer-Schönberger, “Information policy and governance,” *JS Nye und JD Donahue (Hg.) Governance in a Globalizing World, Cambridge*, pp. 330–346, 2000.

[10] J. Zysman and S. Weber, *Governance and Politics of the Internet Economy: Historical Transformation Or Ordinary Politics With a New Vocabulary?* Berkeley Roundtable on the International Economy, 2000.

[11] R. Clarke, “Introduction to dataveillance and information privacy, and definitions of terms,” Aug. 1997. [Online]. Available: http://www.rogerclarke.com/DV/Intro.html

[12] J. M. Fromholz, “European union data privacy directive, the,” *Berk. Tech. LJ*, vol. 15, p. 461, 2000.

[13] Information Security Group of Africa, “Revealing privacy in south africa: What you need to know,” Information Security Group of Africa, Tech. Rep., 2011.

[14] M Law Group, “New draft european data protection regime,” Feb. 2012. [Online]. Available: http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227

[15] S. J. Kobrin, “Safe harbours are hard to find: the trans-atlantic data privacy dispute, territorial jurisdiction and global governance,” *Review of International Studies*, vol. 30, no. 1, p. 111131, 2004.

[16] J. Holvast, W. Madsen, and P. Roth, *The Global Encyclopaedia of Data Protection Regulations*, ser. The Global Encyclopaedia of Data Protection Regulations. Kluwer Law International, 1999, no. v. 1. [Online]. Available: http://books.google.co.za/books?id=TsvQkQEACAAJ

[17] L. B. Movius and N. Krup, “US and EU privacy policy: Comparison of regulatory approaches,” *International Journal of Communication*, vol. 3, p. 19, 2009.

[18] South African Law Reform Commission, “(Project 124) Privacy and Data Protection,” 2005. [Online]. Available: http://www.justice.gov.za/salrc/dpapers/dp109.pdf

[19] Research Gate, “IEEE security and privacy magazine (IEEE SECUR PRIV),” 2013. [Online]. Available: http://www.researchgate.net/journal/1540-7993_IEEE_Security_and_Privacy_Magazine

[20] S. L. Pfleeger, “Security & privacy magazine,” Nov. 2013.

[21] J. Hudson, “2011 IT security review. will 2012 be the year of ubiquitous encryption?” Dec. 2011. [Online]. Available: http://www.securityweek.com/2011-it-security-review-will-2012-be-year-ubiquitous-encryption

[22] J. Lyne, “Year in review: 2011,” 2011. [Online]. Available: http://www.sophos.com/en-us/security-news-trends/security-trends/2011-year-in-review.aspx

[23] F. Rashid, “’Tis the season for security resolutions, not predictions,” Dec. 2012. [Online]. Available: http://www.securityweek.com/tis-season-security-resolutions-not-predictions

[24] G. Eschelbeck, *Sophos Security Threat Report 2014*. Sophos, Dec. 2013. [Online]. Available: http://blogs.sophos.com/2013/12/10/sophos-security-threat-report-2014/

[25] European Union Agency for Network and Information Security, “ENISA threat landscape mid year 2013,” ENISA, Tech. Rep., 2013. [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013

[26] M. Brennan, “Academic impact at the federal trade commission,” *IEEE Security & Privacy*, vol. 10, no. 6, p. 7882, 2012.