Part 1

1 Introduction

1.1 Overview

The right to privacy is commonly recognised as a fundamental human right. The United Nations Universal Declaration of Human Rights (United Nations 1948) and the South African Constitution (Republic of South Africa 1996), in particular, explicitly recognise privacy to be a fundamental right. Information privacy derives from this right and while a formal definition follows in the next chapter, information privacy can be seen as the control individuals have over information that pertains to them. The protection of information privacy, together with the protection of privacy in general[1], is seen as necessary in the maintenance of democracy (Flaherty 1998, p.170-1)(Bygrave 1998) and healthy psychological function (Pedersen 1999).

Information technologies such as networking, databases, data mining and storage media, however, have advanced to the point where storage, sharing and access to personal information facilitates the violation of information privacy to an unprecedented extent (Clarke 1998, p.500)(Head & Yuan 2001, p.150)(Jordaan 2003, p.i)(Smith 1993, p.105). It is therefore now viable for large organisations and governments to violate the information privacy of more individuals with greater ease than in the past. A recent case bears testament to this. In 2010 Google Inc. (Google Inc. 2012a) collected unsecured wireless network traffic without permission in many countries while developing its Street View (Google Inc. 2012b) product. This was termed by the Australian Minister of Communications as "the largest privacy breach in history across Western democracies" (ZDNet 2010).

In response to the risk to information privacy, increased attention has been given to mechanisms that protect information privacy (Ernst & Young 2012). Such mechanisms have been both technological, for example, through so-called privacy enhancing technologies, and legal, via laws designed to protect information privacy. Despite the

1 All references to the term 'privacy' in this thesis refer to the broad concept of privacy, while the term 'information privacy' refers to the more specific concept.

Introduction

increased attention given to protecting information privacy, protective mechanisms have lagged behind the technologies and practices that allow for information privacy violations (Reddy & Venter 2010, p.973). By and large, technological efforts to protect information privacy focus on specific technical problems, such as maintaining anonymity on the Internet. Few efforts have focused on the management of information privacy protection within large organisations. Large organisations, like multi-national companies and government departments, typically hold substantial amounts of information about individuals. Even less work has been done on addressing information privacy protection in organisations in a holistic manner. That is, in a manner that addresses the management of technology, as well as the management of the people and processes involved in processing and storing individuals' information.

At the same time, large organisations that wish to protect information privacy need to be ready to respond in the event that information privacy breaches occur. In many instances large organisations are often mandated by law to protect the information privacy of the individuals whose information they hold (South African Law Reform Commission 2005, ch.8). The protection of private information may entail investigating information privacy breaches to ensure they are not repeated. Investigations may also occur due to the demands of ethical corporate governance (Lau 2001) even if they are not required by law. In order to conduct such investigations, which are likely to involve information technology (IT), digital forensics (DF) is required. In turn, to best conduct a DF investigation a certain amount of preparedness is needed. Such preparedness is the subject of digital forensic readiness (DFR). DFR concerns itself with what is required before a DF investigation starts so that the investigation can be conducted in an optimal manner.

A situation analogous to that of information privacy protection in organisations exists in the field of DFR – very little work has been done on holistic approaches to DFR. Holistic approaches, such as implementation and management frameworks (Reddy & Venter 2009)(Trček et al. 2010), are especially important in large organisations where DFR may involve staff, IT resources and business processes from multiple departments and business units. However, few examples of such frameworks exist. Moreover, fewer

works can be found on approaches to DFR that are specific to the area of information privacy protection. Such work is necessary to understand how best to prepare for investigations of information privacy violations. The management and implementation of DFR within large organisations is also typically carried out under budgetary constraints. No work exists that looks at determining the cost of DFR measures. This is, however, vital to organisations that make implementation and management decisions with respect to cost and fixed budgets.

To summarise the overview thus far, it is evident that there is a dearth of research which concentrates on holistic approaches to the management of both information privacy protection and DFR in large organisations. Additionally, there is virtually no work on: 1) the management of DFR with regard to information privacy protection; and 2) the determination of the cost of DFR measures.

1.2 Problem Statement

This thesis is motivated by a wish to increase the protection of information privacy afforded to individuals by large organisations. Large organisations are the focus of this thesis since large organisations usually hold information about more individuals in society than small organisations or individuals themselves.

Taking cognisance of: the lack of research done in managing information privacy protection and DFR holistically; the near absence of information privacy-specific DFR programmes; and lastly, the lack of research into the costing of DFR measures, this thesis asks the following questions:

- **What is required within large organisations to implement and manage digital forensic readiness for information privacy incidents?** First, it is important to define the term incident. We adapt the definition from Kostina et al. (2009, p.94): an incident is an identified occurrence of a system, service or network state indicating a possible breach of policy or failure of safeguards, or a previously unknown situation that may be relevant to security or privacy. A holistic approach to the management of DFR for information privacy incidents requires an understanding of what is required from a technical and non-technical perspective.

Such an understanding is necessary so that the unique measures required for information privacy, which are likely to be over and above the usual DFR requirements, can be taken into account.

- **How can the cost of DFR measures be determined and used for DFR-related decision making?** Once it has been determined what measures are required for information privacy-specific DFR, large organisations' management will need to make decisions about which measures to use and how to implement the measures. These decisions will be made by considering a number of factors, of which cost and risk are likely to be foremost. Without being able to accurately calculate the cost of such DFR measures, management may be at a disadvantage when making such decisions. Of course, the ability to calculate the cost of DFR measures will also apply to DFR measures that are not information privacy-specific.

- **What are the requirements of a digital forensic readiness management system such that it can be used to assist the management of DFR for information privacy incidents in large organisations?** As mentioned earlier, a holistic approach to the management of information privacy-specific DFR involves coordinating human and technical resources across various departments in an organisation. In a large organisation this may prove to be a formidable task where human error may reduce the effectiveness of DFR and its management. A tool or system to assist in management may therefore help alleviate some of the risk associated with managing DFR in a large organisation. The theoretical requirements for such a system should to be drawn from the literature on DF.

- **How should a digital forensic readiness management system for a large organisation be designed?** Once the theoretical requirements for a digital forensic readiness management system have been determined, .a practical architecture or design for such a system must be developed.

In attempting to answer these questions we hope to address the deficient areas of research mentioned earlier. Also, by providing mechanisms that enable better DF investigations,

we also hope to contribute, in some small measure, to the ultimate aim of this research, namely better protection of information privacy by large organisations.

1.3 Methodology

To answer the questions posed in the problem statement we first performed a rigorous review of the literature on information privacy protection and DFR. Particular attention was given to literature on how information privacy protection and DFR were managed, especially within organisations. We found no work on DFR for information privacy incidents in the literature. Hence, we analysed the literature and extracted the elements considered necessary to manage and implement DFR for information privacy incidents within large organisations – for example, Noblett et al. (2000), Rowlingson (2004) and Wolf (2004). These elements were then used to create a framework that could be used by large organisations aiming to develop a digital forensic readiness capability for information privacy incidents (FORCFIPI).

To address the question of determining the cost of DFR measures we again looked at the literature on cost management for DFR. We found no literature on this topic. We therefore examined the literature on cost management in general and settled on a particular cost management model, namely time-driven activity based costing (TDABC). To establish whether this cost management model could be used for the purposes of managing and reasoning about DFR costs, we conducted statistical simulations. The simulations used both technical and non-technical processes that stemmed from the framework for a digital FORCFIPI developed earlier. This indicated that the cost management model could be used within the context of the framework.

In order to answer the third and fourth questions in the problem statement, we once again reviewed the literature for management tools or systems that are used to manage DFR. Since none were found, we revisited the DFR literature to extract the functional requirements for such a system. From the functional requirements we designed an architecture for a digital forensic readiness management system (DFRMS). A proof-of-concept DFRMS was then developed to validate the DFRMS architecture.

Introduction

Individually each of the questions in the problem statement was answered and contributed to the literature. Each of the contributions can be seen as distinct from the other. That is, they do not concentrate on a single concept. The FORCFIPI is a high-level framework, applying TDABC to DFR is about cost management, and a DFRMS is a technical architecture. The thesis does not take a single, well delineated concept and build upon it in each contribution. In a sense, each of the contributions can be seen as existing in a silo. However, there are links that bind each of the contributions or silos:

- It is necessary to consider cost when managing a FORCFIPI and we show that TDABC can do this.
- The management of DFR, and a FORCFIPI in particular, can be made easier through using a DFRMS.
- Lastly, a DFRMS can help implement TDABC, which in turn allows for better management of cost with respect to a FORCFIPI.

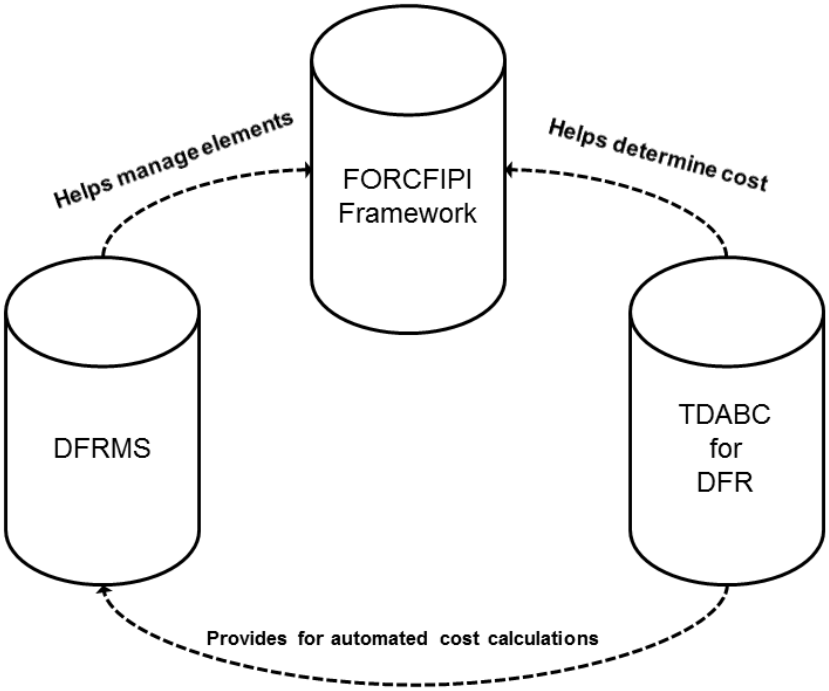

Figure 1 – Diagram showing relationship between contributions.

The relationship between the contributions can be seen in Figure 1. While somewhat distinct, collectively each of these contributions raise the overall protection of

information privacy in large organisations through better, information privacy-specific DFR.

1.4 Terminology

In this thesis we have opted to provide definitions for important terms such as information privacy and digital forensic readiness in the background chapters dedicated to these topics. We do this as numerous definitions for these and related terms are found in the literature and it is easier to explain our choice of definition during a general discussion of these topics and while discussing the other definitions. To aid the readability of this thesis, a glossary of acronyms is included as Appendix A.

1.5 Thesis Layout

This thesis consists of two parts, which together contain 14 chapters. In addition, appendices are given to augment the text. Finally, a bibliography of the references cited in the thesis is provided.

Part 1 of this thesis includes the current chapter and also chapters on the background theory necessary to understand the remainder of the thesis. **Part 2** contains chapters that describe the contributions made in this thesis. Where necessary some of these chapters may also contain small sections that discuss comparative efforts at solving similar problems found in the literature.

The detail of the chapters is as follows:

Chapter 1, the current chapter, introduces this thesis by providing a brief overview. The overview provides some context with regard to information privacy protection, DFR and the state of research in these two areas as it pertains to large organisations. The problem statement for the thesis is also provided in Chapter 1.

Chapter 2 provides an in-depth discussion into the related concepts of privacy and information privacy. The literature on both concepts is reviewed and definitions are discussed. A definition of each concept is adopted for use in this thesis. The legal basis

for information privacy protection is also discussed as well the means used to protect information privacy.

Chapter 3 looks at the field of digital forensics (DF). Various models are presented and relevant terminology is defined. Definitions of DF are discussed and a definition is adopted for use in this thesis.

Chapter 4 examines digital forensic readiness (DFR), a sub-field of DF. DFR is defined and a comprehensive review of the literature is provided. The chapter focuses more on the organisational aspects of DFR and less on technical aspects.

Chapter 5 introduces the time-driven activity based costing methodology known as TDABC. Activity-based costing, from which TDABC is derived, is also presented briefly. Important concepts within TDABC are discussed and an example of TDABC is provided. Chapter 5 is the last chapter in Part 1 of the thesis and marks the end of the background chapters.

Chapter 6 presents a novel framework which can be used by large organisations to develop a digital forensic readiness capability for information privacy incidents (FORCFIPI). The framework identifies the unique elements, such as the policies, processes and procedures, needed by a digital FORCFIPI. It also looks at the relationship between these elements.

Chapter 7 is a short chapter in which the idea of using TDABC as a method to manage costs in a digital FORCFIPI is first proposed then discussed.

Chapter 8 builds on the discussion in Chapter 7 by showing that TDABC can be used for making decisions about costs within a digital FORCFIPI. To show this, a TDABC model is as part of a statistical simulation of a non-technical privacy-specific business process. The simulation environment, the simulation itself and the simulation results are discussed.

Chapter 9 also contains a simulation aimed at showing that TDABC can be used for cost decision making in a FORCIPI. Chapter 9 further presents an analytic technique which allows for so-called ‘what-if’ analyses, which also aid in decision making. The

simulation methodology used in Chapter 8 contains limitations which are addressed in this chapter by performing a more sophisticated simulation in a new simulation environment. The simulation also differs from Chapter 8 as it is of a technical business process.

Chapter 10 leaves the topic of TDABC and puts forward the concept of a digital forensic management system (DFRMS) that assists in the management of DFR in large organisations. The DFMS extends the earlier discussion on the digital FORCFIPI since it assists in the management of a digital FORCFIPI. A comprehensive search of the literature was conducted to determine the functionality necessary for a DFRMS. The results of the review are presented briefly, along with a more thorough exposition of an architecture designed to meet the necessary functional requirements.

Chapter 11 is a brief chapter in which the DFRMS architecture presented in Chapter 10 is discussed. Amongst other things, the discussion looks at how a DFRMS can be used with a digital FORCFIPI. Example scenarios of a DFRMS in use are also provided.

Chapter 12 and **Chapter 13** present our proof-of-concept DFRMS prototype that is based on the architecture in Chapter 11. These chapters detail the workings of the prototype and discuss the various features of the architecture that were implemented in the prototype.

Chapter 14 concludes this thesis and proposes future research that has been identified during the course of this work.

1.6 Conclusion

This chapter provided an introduction to this thesis by presenting an overview, a problem statement and the methodology used to address the problem statement. The layout of the thesis was also described in this chapter.

2 Information Privacy

2.1 Introduction

Information privacy has become increasingly prominent in recent times (Reddy & Venter 2010, p.974). This increased attention is a direct response to advances in information technologies that are potentially detrimental to the information privacy of individuals. Through such advances it is now possible to store, access and transmit larger volumes of information about more individuals than ever before (Clarke 1998). A number of mechanisms, both of a technical and non-technical nature, have been put forward to help reduce the harm to the information privacy of individuals (Borking & Raab 2001)(Gritzalis 2004, p.11-17).

Despite the increased prominence of information privacy, there is no single, commonly accepted definition of the concept. Indeed, the broader concept of privacy itself does not enjoy consensus with regard to a definition (Solove 2006). The purpose of this chapter, therefore, is to: review the concepts of privacy and information privacy, including the relevant South African and international law; adopt definitions of these concepts for use in this thesis; and, discuss the technical and non-technical measures aimed at protecting information privacy.

2.2 What is Privacy?

Privacy is a word that is used commonly in everyday language. It has been used in the English language since at least the 15th century (Bonner 2002, p.111), however, as a concept, it has no single, universally accepted definition. In fact, there are sufficiently many definitions of the concept that it is said to "suffer an embarrassment of meanings" (Solove 2006). Kasper (2005, p.72) observes that authors writing in different subject areas offer definitions of privacy that are too narrowly specified for their subject areas. Westin, an author of foundational work on privacy, is cited in Gellman (1998) as being of the view that privacy has a multitude of meanings due to the subjective nature of the concept. Westin believes that the definitions espoused are a function of, *inter alia*, the values and interests of those that espouse them (Gellman 1998, p194). A single,

commonly accepted definition of privacy is therefore impossible because values and interests vary (Gellman 1998). We concur with Westin's view since we believe it is self-evident that the values and interests of individuals differ. Moreover, research on culture and privacy shows that cultural values, at the minimum, influence an individual's perception of privacy (Cullen & Reilly 2007)(Kitiyadisai 2005)(Olinger et al. 2005). Westin's view also offers a possible explanation of Kasper's observation insofar as authors' interests may rest in their own fields, resulting in definitions of privacy that are biased towards their fields.

In this section we look at definitions of privacy in an attempt to obtain a clearer understanding of the concept. We also discuss the legal basis for the right to privacy.

2.2.1 Definitions of Privacy

Much has been written on the nature of privacy. Most of the contributions to the literature on privacy stem from academic disciplines such as law, social science and philosophy (Fischer-Hübner & Lindskog 2001). In the nineteen eighties, authors such as McCloskey (1980) and Parent (1983) looked at the concept of privacy and identified various classes of definitions. McCloskey identified ten such classes, while Parent identified five. Each class contained definitions, which had at their core common values, beliefs or criteria regarding the nature of privacy. It is important to note that definitions in these classes were not always mutually exclusive. In other words, it is possible for definitions of privacy from two classes to hold without contradicting each other on any fundamental points.

In 2002, Solove (2002) performed an exercise similar to McCloskey and Parent. He identified six classes of privacy definitions. We base our discussion of privacy definitions on Solove's work because it is more recent and covers the work done in the decades subsequent to McCloskey and Parent. The six classes Solove defines are as follows: 1) the right to be let alone; 2) limited access to the self; 3) secrecy; 4) control over personal information; 5) personhood; and 6) intimacy.

2.2.1.1 The Right to Be Let Alone

The definition of privacy as the right to be let alone is one of the earliest and best known scholarly definitions (Leino-Kilpi et al. 2001, p.664). It stems from the seminal article in 1890 by Warren and Brandeis entitled *The Right to Privacy* (Warren & Brandeis 1890). Definitions of privacy that subscribe to Warren and Brandeis' notion of privacy hold that privacy is the right to a state of solitude or seclusion from others (Solove 2002).

2.2.1.2 Limited Access to the Self

In the limited access to the self view, privacy is about individuals deciding the extent to which they want to interact with others. (Solove 2002, p.1102-5)(Parent 1983, p.344-345). The definition of privacy as the right to solitude is not negated, however, as solitude is viewed purely as one state in a continuum of states individuals may desire. Privacy, rather, is seen as a boundary regulation processes in which individuals dynamically control their boundaries and allow more or less access to themselves by others (Samarajiva 1998, p.283)(Altman 1976).

2.2.1.3 Secrecy

Definitions in the secrecy class describe privacy as the right of individuals to hold information about themselves from others. Posner, a scholar of privacy, holds this view. He is often cited in the literature, for example by Solove (2002, p.1105-6), Introna (1997, p.263-4) and Hirshleifer (1980). Posner's definition of privacy as secrecy is, in fact, stricter as he describes privacy as the right of an individual "to conceal discreditable facts about himself" (Solove 2002, p.1106). The narrow definition of privacy as secrecy is not commonly advocated by privacy scholars and is refuted, for example, by Parent (1983), Introna (1997, p.263-4) and Solove (2002, p.1109).

2.2.1.4 Control Over Personal Information

The focus of this class of definitions is on information and the exercise of control over information. Westin's widely cited definition of privacy typifies definitions in this class. He defines privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to

others" (Westin 1970, p.7). The emphasis on information, to the exclusion of other aspects of privacy, such as physical or bodily privacy contrasts this class of definitions with definitions in the 'limited access to self' category, which also encompass physical privacy (Solove 2002, p.1110).

2.2.1.5 Personhood

The term 'personhood' was defined by privacy scholar Freund as "those attributes of an individual which are irreducible in his selfhood" (Solove 2002, p.1116). Definitions in this category address different attributes referred to in Freund's definition of 'personhood'. Attributes such as individuality, dignity, autonomy, and personality are all included by various authors espousing definitions in this class (Solove 2002, p.1116)(McCloskey 1980, p.29). The concept of privacy is seen, in these definitions, as that which protects against an individual from harm to one or more of these attributes. These attributes are seen here as necessary for the normal functioning of individuals. The definitions in this class are often used by authors offering definitions in the other classes to illustrate the damage done though loss of privacy (Solove 2002, p.1116).

2.2.1.6 Intimacy

In the intimacy class of definitions, privacy is viewed as a form of intimacy (Solove 2002, p.1121), or as "control over the intimacies of personal identity" (Parent 1983, p.342-3). Specific emphasis is placed on the control of information and the limitation of access as these relate to interpersonal relationships (Solove 2002, p.1121). The underlying premise in these definitions is that such control and limitation is necessary for human relationships to develop and function.

It is clear from the preceding discussion, that there are many approaches to defining privacy. By basing the review of the literature on Solove's six classes we have covered the field in a broad manner. It should be noted, however, that within each class there are a number of different definitions, and indeed, there are definitions that will not fit easily into any one of the six classes. The breadth and depth of the literature, though, makes a more comprehensive treatment of the subject here impractical.

2.2.2 Privacy – Adopting a Definition

In this section we advance a definition of privacy for use in this thesis. That is, any further reference to privacy shall, by default, refer to the definition put forward here. The definition and discussion that follows is based on the review of privacy definitions in the previous section.

We adopt the view that privacy is a fundamental human right because it is a basic human need. McCloskey (1980, p.34) points to a lack of empirical evidence for such a view, however, subsequent empirical research undertaken by Pedersen (1999) affirms the view that privacy is a basic need and that it is required for healthy psychological functioning. Moreover, privacy is required for the free political activity that is necessary in a democracy (Clarke 2006)(Laudon 1996, p.92)(Margulis 2003, p.246). The content of political meetings, discussions and organisational activities, for example, should be undertaken free from improper surveillance by political opponents or the state.

We therefore formulate the following definition of privacy as a definition:

Privacy is the right of individuals to control both information about themselves and their boundaries during interactions with others.

This definition is a combination of Westin's definition (Westin 1970, p.7), from the 'Control Over Personal Information' (COPI) class of definitions, and Samarajiva's definition (1998, p.283), from the 'Limited Access to the Self' (LATTS) class. The rationale for combining these two definitions is that the combined definition incorporates definitions from the other classes identified by Solove (2002); or, where it does not, it allows for privacy to be maintained according to the definitions in the other classes. As mentioned in Section 2.2.1.2, the LATTS class of definitions incorporates the 'Right to be Let Alone'. Similarly, the COPI class of definitions can be seen to incorporate definitions in the 'Secrecy' class since control over information can imply secrecy. The definition we put forward does not, however, suffice as a definition of privacy under the 'Personhood' and 'Intimacy' classes. The definition can still, nevertheless, be used to ensure that privacy is protected under these classes. For example, if an individual can

control information about themselves and their boundary conditions, they may be able to ensure that none of the attributes of personhood may be harmed.

It should be noted that Samarajiva (1994) describes his definition, mentioned in passing earlier in the LATTS class, as including the inflow and outflow of information. The question thus arises: Why include Westin's definition? The answer is that the reference to the flow of information is not explicit in the wording of Samarajiva's definition. Furthermore, Samarajiva's definition does not take into consideration the control of information after outflow. Westin's definition, which is explicit about the control of information, is thus used.

2.2.3 The Right to Privacy

The previous sections discussed privacy as an abstract concept. Although there is disagreement about whether privacy ought to be a right, or merely a claim or interest (Clarke 2006), legal instruments do exist which give effect to a right to privacy. In this sense, privacy is less abstract and more concrete in that it can be enforced by law. The legal definitions and interpretations of privacy vary from country to country. We do not provide an in-depth discussion of these definitions and interpretations. Rather, we list some of the prominent legal instruments that grant a general right to privacy in South Africa and internationally. These legal instruments are listed primarily to establish the basis for the more specific right to information privacy, which is discussed later in this chapter. Legal protections for information privacy in particular, are also dealt with later in this chapter.

2.2.3.1 International Privacy Rights

Internationally, the right to privacy is recognised as a fundamental human right by the United Nations Universal Declaration of Human Rights (UNDHR). The UNDHR was adopted in 1948 by the General Assembly of United Nations. Article 12 of the UNDHR states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations 1948). The UNDHR is not a treaty, however, and is therefore not legally binding on the member

nations of the United Nations (Dugard 2006, p.314). While not binding, the UNDHR has created a *de facto* standard regarding the human rights (Buergenthal 1988, p.6-9) of individuals and has served as the foundation of the field of international human rights law (Lindgren Alves 2000, p.478).

In Europe, the Council of Europe imposes the Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe 1950) on its forty seven member states. The convention is also known as the European Convention on Human Rights (ECHR). Article 8 of the ECHR addresses privacy and states, *inter alia*, that "everyone has the right to respect for his private and family life, his home and his correspondence" (Council of Europe 1950).

In the Americas, the Organisation of American States (OAS) adopted the American Convention on Human Rights (ACHR). Article 11 of the ACHR (Organisation of American States 1969a) describes a right to privacy that is similar in wording to the ECHR. Not all countries in the Americas have ratified the ACHR (Organisation of American States 1969b) and are therefore not bound by it. Most notable amongst those that have not ratified the convention are the United States of America (USA) and Canada.

In the USA the national constitution contains no explicit right to privacy (Beaney 1962, p.214). The constitutions of a number of states do, however, provide for an explicit right to privacy and there exist "dozens of federal privacy statutes, and hundreds of state privacy statutes" (Solove 2006, p.483).

In Africa, the regional human rights system is underpinned by the African Union's African Charter on Human and Peoples' Rights (ACHPR) (Douglas 2000, p.134). The ACHPR does not contain an explicit right to privacy (Organisation of African Unity 1986). In the next section the South African view on the right to privacy is discussed. It will be seen that the South African view on privacy differs from the view found in the ACHPR.

2.2.3.2 Privacy Rights in South Africa

In South Africa, the Constitution is "the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled" (Republic of South Africa 1996, §1.2). The right to privacy is considered a fundamental human right and is provided for explicitly in the Bill of Rights of the Constitution. Section 14 of the Bill of Rights states:

"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." (Republic of South Africa 1996, §2.14)

The South African Constitution is an act of parliament or statute. It is therefore an example of a statutory law, or a law that is a written, codified act of the legislature (Garner 1999, p.270). In South Africa, the right to privacy is also protected by the common law (South African Law Reform Commission 2005, ch.2, p.3). The common law refers to law that, in its practice, relies on the precedent of judicial decisions and not on acts of legislature (Martin 2006, p.104). In terms of the common law, the notion of privacy is not explicitly defined as it is in the Constitution. Rather, it develops from the judgements passed on cases involving privacy that have been tried under the common law.

Other statutes also protect the right to privacy, but these pertain more to information privacy, and, as such are discussed in the next section.

2.3 What is Information Privacy?

A number of authors have divided the concept of privacy into various dimensions. Burgoon and Parrot et al., who are cited in Leino-Kilpi et al. (2001, p.664), and Clarke (2006) divide privacy into four dimensions. Rosenberg and Holvast are individually cited by Fischer-Hübner and Lindskog (2001, p.3) as dividing privacy into three

dimensions. While the aforementioned authors differ slightly on what the exact dimensions of privacy are, they are unanimous in their inclusion of information privacy as a dimension. Information privacy can therefore be considered a specific form of the larger concept of privacy. The other dimensions of privacy identified by the authors above are not relevant to this work and are therefore not discussed further. For the sake of completeness, however, they are shown in Table 1.

As previously mentioned, information privacy does not have a single, commonly accepted definition. From our review of the literature we note that the definitions of information privacy do not usually differ widely regarding the fundamental meaning of the concept. This is because the focus on information negates the other aspects of privacy, such as the social, psychological or physical aspects. The definitions, therefore, generally, relate to the control of personal information. As such, the number of different definitions is fewer than in the case of privacy as a whole. In the following section we give examples of some definitions and discuss them.

Table 1 – Privacy dimensions

Burgoon & Parrot et al.		**Clarke**		**Rosenberg & Holvast**	
Social Privacy	Physical Privacy	Privacy of Person	Privacy of Personal Behaviour	Territorial Privacy	Privacy of Person
Informational Privacy	Psychological Privacy	Privacy of Personal Communications	Privacy of Personal Data[2]	Informational Privacy	

2.3.1 Definitions of Information Privacy

Westin's definition of privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin 1970, p.7) is often also cited as a definition of information privacy. This is due to the emphasis on the control of personal information in Westin's definition (recall that Westin's definition of privacy belongs in the Control Over Personal Information class of privacy definitions as discussed in Section 2.2.1.4). Westin's definition is seminal as it forms the crux of most of the definitions of information privacy that followed it.

2 The privacy of personal data is synonymous with the term 'information privacy' (Clarke 2006).

Culnan and Bies as cited in Rapp et al. (2009, p.54), for example, posit a definition similar to Westin's definition. They define information privacy as the "ability of individuals to control the terms under which their personal information is acquired and used". This definition, while similar to Westin's, differs on three points. Firstly, Culnan and Bies see information privacy as an ability rather than a claim. Secondly, unlike Westin's definition that refers to groups or institutions, Culnan and Bies refer only to individuals. Thirdly, Culnan and Bies define information privacy in terms of the control over the acquisition and use of personal information, rather than the control over the communication of personal information. With regard to the first difference, Culnan and Bies see information privacy as a practical concept. In their view it is an ability that can be exercised. Conversely, Westin views information privacy as a claim. A claim is less practical as one may have a legal or moral claim but no practical ability to exercise the claim. The second difference is also important as Culnan and Bies's definition excludes groups or institutions from exercising information privacy. The last difference is also significant. Westin's definition does not consider the use of information after it has been legitimately communicated to another. It is more concerned with information being communicated to others. Westin's definition does not consider the case of communicating private information to another party for a specific purpose and having that party use it for different purpose.

Wasserstrom, cited in Foxman and Kicoyne (1993, p.106), defines information privacy as "the kind and degree of control that a person ought to be able to exercise in respect to knowledge or the disclosure of information about himself or herself". Wasserstrom's definition contains measures of both Westin's definition and Culnan and Bies's definition. It is similar to Culnan and Bies's because it refers to information privacy as a "kind and degree of control", in other words, an ability similar to the 'ability' Culnan and Bies refer to in their definition. The use of the words "ought to" in Wasserstrom's definition imply that the ability should be exercised in terms of some moral or legal claim. This is consistent with Westin's definition of information privacy as a claim. Wasserstrom's definition, like Culnan and Bies's, also defines information privacy with regard to individuals and not groups and institutions like Westin.

Smith (1993, p.106) defines information privacy as a "condition of limited access to identifiable information about individuals". Smith's definition is provided here as an example of a definition that does not fit in with the usual definitions that define information privacy purely in terms of control over information. Smith defines information privacy as a condition rather than an ability or claim. Moreover, the condition is characterised by limited access to personal information. This definition, thus, concentrates more on access than control. While limited access implies a degree of control over the information, this control is limited purely to accessibility – it does not consider control over the dissemination or use of personal information. In this regard it is atypical of information privacy definitions.

In the discussion thus far the definitions by Westin, Culnan and Bies, and Wasserstrom illustrate typical definitions of information privacy, and the type of points by which they typically vary. Smith's definition conveys that, even though most definitions centre on control of information, definitions are not uniform in this regard.

2.3.2 Information Privacy – Adopting a Definition

In this section we present a working definition of information privacy for use in this thesis. As with the definition of privacy in Section 2.2.2, any further reference to information privacy shall, by default, refer to the working definition.

We have shown in Section 2.3 that information privacy is a more specific form of the broader concept of privacy. Any definition of information privacy, therefore, should follow from, or be consistent with, a definition of privacy. The definition of information privacy we state here thus follows from our definition of privacy. We define information privacy so:

Information privacy is the right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination and veracity of information about themselves.

This definition is derived from Clarke's definition of information privacy as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves" (Clarke 2006).

The definition we posit differs from Clarke's as we view information privacy as a right and not an interest. This follows from our definition of privacy as a fundamental human right. Also, rather than use the term 'handling' as a general term regarding how information is dealt with, we specify that information privacy refers to acquisition, access, use, dissemination and veracity.

2.3.3 The Fair Information Principles

The Fair Information Principles (FIPs) are a set of guidelines for dealing with personal information. They provide guidance on how to effect the right to information privacy by defining what should and should not be done with personal information.

The FIPs were originally published as four principles in a 1973 report by the United States Department of Health, Education, and Welfare (Federal Trade Commission 2000, p.3-4). The number of principles, however, has since been expanded upon by other organisations. For instance, the Organisation for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Organisation for Economic Cooperation and Development 1980), known as the OECD Guidelines, contains eight principles. In this thesis we use the FIPs that are contained in the OECD Guidelines. Other documents may vary in the number of principles they contain. For example, the United States Federal Trade Commission lists five FIPs (Federal Trade Commission 2007). We use the OECD Guidelines, though, as they are comprehensive.

The FIPs from the OECD Guidelines are quoted below (Organisation for Economic Cooperation and Development, 1980). In the context of our work, the term 'data' used in the text of the OECD Guidelines is synonymous with the term 'information'. The term 'data subject' is an individual about whom the data refers.

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the previous principle] except:
  a) with the consent of the data subject; or
  b) by the authority of law.

- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation Principle:** An individual should have the right:
  a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

- **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

In the next section we discuss how the right to information privacy is protected in the law.

2.3.4 Information Privacy in the Law

Information privacy can be considered a right under the more general right to privacy (South African Law Reform Commission 2005, ch.1, p.2) that was discussed in Section 2.2.3. A number of countries that recognise the right to privacy also provide legal protection for information privacy. Globally, laws dedicated to protecting information privacy are based on the FIPs from the OECD Guidelines (Bonner 2002, p.121-3)(Gellman 1998, p.194). In addition to laws that focus on information privacy, other laws whose primary focus lies elsewhere, may also impact information privacy. Laws regarding the credit rating of consumers are an example of such laws. In this section we discuss these legal protections available both internationally and in South Africa.

2.3.4.1 International Information Privacy Laws

Throughout the world two predominant approaches to the protection of information privacy exist: self-regulation and government regulation. Given that there are many countries with information privacy legislation, we restrict our discussion to the approaches taken by the United States (US) and the European Union (EU) since they exemplify the two approaches.

Information Privacy

In the EU, information privacy, is governed by the European Union Directive on the Protection of Personal Data (European Parliament 1995), or EU Data Directive. The EU Data Directive considers information privacy a part of the fundamental human right to privacy (European Parliament 1995, art.1). It contains a set of FIPs based on the FIPs in the OECD Guidelines (Bellman et al. 2004, p.314) and requires member states of the EU to each adopt information privacy laws that are consistent with the FIPs (Walczuch and Steeghs 2001, p.146). These laws affect all of society, including individuals, organisations and the state itself. Each member state is further required to have an independent supervisory authority, such as a data protection commission, that has significant powers regarding information privacy. A supervisory authority is required to: monitor the application of laws; consult with government; receive complaints from the public; conduct investigations; intervene in the processing of personal information, for example, by banning certain processing; and finally, institute legal proceedings where it deems the law has been violated (European Parliament 1995, art.28). Information privacy is therefore strictly regulated through the law and the workings of the supervisory authorities. This makes the EU exemplary of the government regulation approach.

In the US there is no overarching federal or national information privacy law that encompasses the federal and state governments, individuals and organisations. Instead, federal information privacy laws have been adopted in a reactive manner as issues arise (Bonner 2002, p.134)(Walczuch & Steeghs 2001, p.145). Most federal laws target specific sectors (Bellman et al. 2004, p.315), for example, the: Health Insurance and Portability Act that targets the health sector (California Office of Privacy Protection 2010). A federal Privacy Act also exists that regulates the federal government's use of individuals' personal information through basic FIPs (Bonner 2002, p.133)(California Office of Privacy Protection 2010). The US approach is to allow industries to voluntarily regulate themselves (Bellman et al. 2004, p.145)(Federal Trade Commission 2000, p.6-7).

Oliver-Lalana (2004, p.114) articulates the difference between the two types of approaches: "Data protection is approached in Europe as a fundamental right prevailing *prima facie* over economic interests, whereas in the United States it is rather a mere

commercial issue, so that companies claim ownership over customer information and tend to do with it as they do with any other company asset".

2.3.4.2 South African Information Privacy Laws

At the time of writing, South Africa has no laws or statutes dedicated to information privacy. As mentioned earlier in Section 2.2.3.2, the right to privacy is protected by the common law. Depending on circumstances, information privacy, can also be protected by the common law. Pursuant to the constitutional right to privacy, the South African Law Reform Commission (SALRC) was tasked with investigating privacy and data protection in 2003 and drafting appropriate legislation (South African Law Reform Commission 2009, p.1). The SALRC completed its investigation in February 2009 (South African Law Reform Commission 2009, p.1) and a Bill was tabled in the national parliament on the 25th of August 2009 (Parliament of South Africa 2009).

Table 2 – Laws with an impact on information privacy

Name of Act	Relevant Sections	Scope
Promotion of Access to Information (Republic of South Africa 2000)	Entire Act	Offers individuals access to information about themselves.
National Health Act (Republic of South Africa 2004)	§13-17	Contains provisions regarding health records of individuals.
National Credit Act (Republic of South Africa 2005)	§67-73	Deals with the credit records of consumers.
Electronic Communications and Transactions Act (Republic of South Africa 2002)	§45, §50-51	Governs the use of all types of electronic communication systems.
Regulation of Interception of Communications and Provision of Communication-related information Act (Republic of South Africa 2002)	Entire Act	Regards the interception of communication though any medium.
Financial Intelligence Centre Act (Republic of South Africa 2002)	§21-26, §40-41	Aimed at controlling money laundering and other financial crime.
Consumer Protection Act (Republic of South Africa 2008)	§11-12	Extends the right to privacy to include the right to not receive direct marketing

The Bill is entitled 'Protection of Personal Information Bill' and proposes a government regulation approach as found in the EU Data Directive. The Bill contains the same set of eight FIPs listed in the OECD Guidelines and also proposes an Information Protection

Regulator that is similar in function to the supervisory authorities as mandated by the EU Data Directive. At the time of writing, however, the Bill has not been enacted into law.

In South Africa, a number of non-privacy-specific laws contain provisions that impact information privacy. These laws are listed in Table 2. If enacted in its form at the time of writing, the Protection of Personal Information Bill will amend the following Acts to ensure consistency in the law: Promotion of Access to Information Act, Electronic Communications and Transactions Act, and the National Credit Act.

2.3.5 Protection of Information Privacy

There are a number of ways in which information privacy is protected. These range from the laws mentioned in the previous sections, to specific technical measures such as the encryption of personal information. The term 'privacy enhancing technologies' (PETs) has no widely accepted definition (META Group 2005, p.4). It is often used in the literature to refer to technical measures for protecting information privacy, for example, in Gritzalis (2004, p.11-16) and Borking and Raab (2001, p.1). Burkert (1998, p.125) however, takes a wider view of the term and defines PETs as "technical and organisational concepts that aim at protecting personal identity". We adopt Burkert's view because it allows us to classify the various means of protecting information privacy as different forms of PETs, such as in Reddy and Venter (2007, 2010). In Reddy and Venter (2007) PETs are classified as either organisational PETs or technical PETs. Organisational PETs are further classified as either application-level or high-level PETs. The classification can be seen in Figure 2. PCMMs in Figure 2 refers to privacy capability maturity models, which are described later in this section.

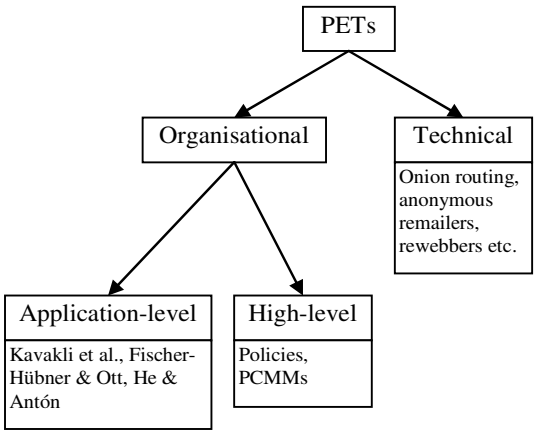

Figure 2 – A classification of PETs from Reddy and Venter (2007, p.3)

Technical PETs are designed to solve specific technical problems, mostly with regard to the maintenance of privacy on public networks such as the Internet. This is usually accomplished by using distributed system architectures, network protocols, and software tools that ensure anonymity (Kavakli et al. 2006, p.146). The defining feature of these PETs is that they do not take organisational context into consideration (Kavakli et al. 2006, p.144). Onion routers, anonymous re-mailers and rewebbers are all examples of technical PETs. Table 3 shows these and other technical PETs and explains their function.

Table 3 – Examples of Technical PETs

Technical PET	Description
Anonymous re-mailer	"Anonymous re-mailers allow e-mail messages to be sent without revealing the identity of the sender" Gritzalis (2004, p.13)
Rewebber	"A rewebber is a PET used for anonymously surfing the Internet" Gritzalis (2004, p.14)
Onion routing	"Onion routing…is a flexible communications infrastructure that is resistant to eavesdropping and traffic analysis. It provides anonymous, bi-directional and near real-time connections…" Gritzalis (2004, p.14)
Crowds	"Crowds…is a system for protecting the anonymity of a user while browsing the Web" Gritzalis (2004, p.15)
Hordes	"Hordes is a protocol designed for utilising multicast communication for the reverse path of anonymous connections…[it achieves] not only anonymity but also sender unlinkability and unobservability" (Kavakli et al. 2006, p.143)
GAP	GNUnet's Anonymity Protocol "achieves anonymous data transfers" and is "customised to the functionality of a peer-to-peer network" (Kavakli et al. 2006, p.143)

Organisational PETs, on the other hand, are designed to protect information privacy within an organisation. This is a much broader class of PETs as the class may include organisational privacy policies and even disciplinary policies. Organisational PETs, as previously mentioned, consist of application-level and high-level PETs. Application-level organisational PETs (ALO PETs) are named so because they are primarily designed to include access to and control of private information into an organisation's information systems (Fischer-Hübner & Ott 1998)(He & Antón 2003)(Kavakli et al. 2006). The access or control afforded to staff in the organisation is usually a function of the organisation's privacy policy and any applicable legal restrictions. If an organisation's privacy policy states, for example, that staff in the marketing department may not have access to customers' banking details, these PETs will prohibit them from gaining such access. ALO PETs usually utilise requirements engineering techniques, various access control methods, or some combination of both, to take organisational context into account. ALO PETs help mitigate the risk of private information on information systems being accessed by inappropriate individuals. They also help mitigate the risk of inappropriate flow of private information through an organisation's information systems. Examples of application-level organisational PETs include:

- Kavakli et al.'s 'PriS' conceptual framework (2007), which takes the privacy requirements and goals of a business into account when determining system requirements – it uses requirements engineering techniques.
- Fischer-Hübner and Ott's implementation of an access control-based PET (1998) that enforces privacy policies for data access and usage.
- He and Antón's framework (2003) which uses role engineering (a form of requirements engineering) to specify roles for a role-based access control approach to modelling privacy requirements within an organisation's applications.
- Karjoth and Schunter's privacy policy model (2002). It makes use of a privacy control language to enforce organisational privacy policies.
- Casassa Mont's obligation management model (2004) and obligation management system (2006) for dealing with an organisation's information privacy obligations to its data subjects.

High-level organisational PETs (HLO PETs) are implemented at a high level within an organisational hierarchy and are pervasive throughout the organisation. That is, HLO PETs affect staff at all levels of an organisation, the organisation's choice of technology and its use of technology. An organisational privacy policy is an example of an HLO PET as it would typically describe the appropriate use of data subjects' private information by all staff. Privacy capability maturity models (PCMMs) (Reddy & Venter 2007)(Hahn et al. 2006) are also examples of HLO PETs. A PCMM can be defined as a reference model of mature information privacy protection processes and associated practices used to improve and appraise an organisation's capability to protect the information privacy of its data subjects (Reddy & Venter 2007, p.2). PCMMs are implemented with a top-down approach in an organisational hierarchy and their effects are pervasive, hence PCMMs satisfy the definition of a HLO PET.

2.4 Conclusion

This chapter reviewed the concept of information privacy. Since information privacy derives from the broader concept of privacy, this broader concept was reviewed to provide a conceptual foundation. Privacy has numerous definitions; however, for the purpose of this thesis privacy can be defined as the right of individuals to control both information about themselves and their boundaries during interactions with others. The right to privacy is recognised as a fundamental human right internationally through various declarations and conventions. In South Africa the right to privacy is also explicitly recognised as a fundamental right in the Constitution and is also protected under the common law.

Information privacy, too, does not have a universally accepted definition. We define information privacy in this thesis as the right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination and veracity of information about themselves. The practical means by which to effect this right are contained in the Fair Information Principles (FIPs). Information privacy is protected by law in many countries around the world, predominantly through two types of enforcement: self-regulation and government regulation. In either approach, the FIPs form the basis of most information privacy law. At the time of writing this, South Africa

has no specific legislation that governs information privacy, however, information privacy is protected by the common law. A bill has been tabled in the South African parliament that proposes legislation similar to the EU but the bill has not been passed at the time of writing.

Information privacy can be protected through privacy enhancing technologies (PETs). By defining PETs as technical and organisational concepts that aim at protecting personal identity, PETs can be classified as organisational and technical PETs. Technical PETs usually solve specific technology-related problems and do not take organisational context into consideration. Organisational PETs, on the other hand, are designed to consider the organisational setting and usually apply throughout an organisation.

The definitions of privacy, information privacy, PETs, as well as information on the FIPs and information privacy laws are provided in this chapter as they are referenced later in the thesis.

3 Digital Forensics

3.1 Introduction

Digital devices, such as computers, personal digital assistants (PDAs), cellular phones and even routers have become ubiquitous in many societies (Abdullah et al. 2008, p.215). As a result, digital devices are increasingly the subject of forensic investigations (Haggerty & Taylor 2006, p.14). Such forensic investigations are called digital forensic investigations and form part of the field of digital forensics (DF). We define digital forensics as follows:

The scientific discipline that concerns itself with the preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary or root cause analysis, or the anticipation of unauthorised actions that may be disruptive to planned operations (Kruse & Heiser 2001, p.1)(Palmer 2001, p.17).

Any number of scenarios involving digital devices can conceivably give rise to investigations that make use of DF. In practice, however, DF is typically used in two contexts: (1) criminal investigations; and (2) internal investigations by organisations into incidents such as computer security breaches, disputes or equipment failures. The two contexts are not necessarily mutually exclusive as internal organisational investigations may uncover criminal activity and the resultant evidence used in a criminal court. In this thesis we are more concerned with DF in an organisational setting. A significant difference between DF in a criminal investigation and DF in an internal organisational investigation is that, generally, organisations conducting internal investigations have the opportunity to proactively collect potential digital evidence before an incident occurs (Rowlingson 2004, p.1). Criminal investigations, on the other hand, often occur in environments where the proactive collection of potential digital evidence is not possible.

The proactive measures taken before an investigation are the subject of digital forensic readiness (DFR). The purpose of this chapter is to discuss DF in order to place the concept of DFR in context in the next chapter.

The remainder of this chapter is structured as follows: first, definitions of digital forensics are discussed and then various models of the digital forensic process found in the literature are presented.

3.2 Digital Forensics

In the preceding section we put forward a definition of digital forensics that is a conjunction and slight adaptation of definitions from Kruse and Heiser (2001, p.1) and Palmer (2001, p.17). As in the case of privacy, however, there is no single, commonly accepted definition of DF. A number of definitions exist in the literature. Examples of such definitions are given in the following bullet list:

- The processes or procedures involving monitoring, collection, analysis and presentation of digital evidence as part of 'a priori' or 'post-mortem' investigations of computer misuse (Hannan et al. 2003, p.2).
- The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable (McKemmish 1999, p.1).
- Computer forensics deals with identifying, preserving, recovering, analysing, and documenting computer data allegedly used in crimes committed using computers (Gottschalk et al. 2005, p.147).
- Computer forensics is the science that is concerned with the relation and application of computers and legal issues (Kuchta 2000).

Two common themes are prevalent in the definitions listed in the bullet list above. First, definitions such as those by McKemmish, Gottschalk et al., and Kuchta make explicit mention of a legal or criminal context. The definition we put forward takes these contexts into consideration implicitly through the reference to evidentiary analysis. We believe that DF can also be used also for root-cause analyses, often in contexts that are completely divorced from the legal or criminal contexts.

Another distinction between the definition we put forward earlier and the definitions above is the use of the term 'computer forensics'. Gottschalk et al. and Kuchta use this term in their definitions above. 'Computer forensics' is an historical term from the late nineteen eighties that was originally used to refer to the forensic examination of stand-

alone computers (Yasinsac et al. 2003, p.15). Some authors, such as Grobler and Louwrens (2006), hold the view that due to the multitude of digital devices that exist in addition to computers, "computer forensics has become a subset of DF" (Grobler & Louwrens 2006). Other authors, such as Reith et al. (2002, p.2) believe the term 'computer forensics' has expanded to include the forensics of all digital technology (Reith et al. 2002, p.2). We follow Grobler and Louwrens and use the term digital forensics to refer to all digital devices rather than simply computers.

We define digital devices to be synonymous with digital objects as defined by Carrier and Spafford (2004, p.2), namely as a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a process. Digital data is also defined per Carrier and Spafford's definition as data represented in a numerical form. While digital data is typically encoded in a binary format, this is not required to satisfy the definition. These definitions of digital devices or objects and digital data are commonly accepted definitions in DF (Carrier & Spafford 2004, p.2).

Numerous models, frameworks and methodologies have been developed to capture or specify the phases or steps in a DF investigation (Grobler & Louwrens 2006)(Perumal 2009, p.38-40). In the next section we discuss these models.

3.2.1 The Digital Forensic Investigation Process

Digital forensic investigations typically follow a process that can be divided into a number of phases. The process by which a DF investigation is conducted is so central to DF that some authors define DF itself as a process or processes – for example, the definitions given by Hannan et al. (2003, p.2) and McKemmish's (1999, p.1) in the previous section. Given that DF is a relatively new science (Reith et al. 2002, p.2)(Yasinsac et al. 2003, p.15), many competing models, frameworks and methodologies have been proposed that specify the different phases in a DF investigation. Table 4 below from Perumal (2009, p.39) shows a partial list of models. We discuss some of these models in this section.

Table 4 – Digital forensic investigation models from Perumal (2009, p.39)

Model Name	Authors	Date	Nr of Phases
Computer Forensic Process	M. Pollitt	1995	4
Generic Investigation Process	Palmer	2001	7
Abstract Model of the Digital Forensic Procedures	Reith, Carr & Gunsh	2002	9
An Integrated Digital Investigation Process	Carrier & Spafford	2003	17
End To End Digital Investigation	Stephenson	2003	9
Enhanced Integrated Digital Investigation Process	Baryamureeba & Tushabe	2004	21
Extended Model of Cyber Crime Investigation	Ciardhuain	2004	13
Hierarchical, Objective Based Framework	Beebe & Clark	2004	6
Event Based Digital Forensic Investigation Framework	Carrier & Spafford	2004	16
Forensic Process	Kent Chevalier, Grance & Dang	2006	4
Investigation Framework	Kohn, Eloff ,& Oliver	2006	3
Computer Forensic Field Triage Process Model	Roger, Goldman, Mislan, Wedge & Debota	2006	4
Investigation Process model	Freiling & Schwittay	2007	4

3.2.1.1 Pollitt's Computer Forensic Process

One of the earliest works describing the DF investigation process is by Pollitt in 1995 (Pollitt 1995). Pollitt describes the DF investigation process as comprising of four phases. He also defines four transitions that transform digital evidence from physical media, such as a hard disk, to evidence that is presentable in a court of law. The process presented by Pollitt takes the implicit view of DF as part of a legal process and does not consider DF as part of root-cause analyses.

The four steps identified by Pollitt are: acquisition, identification, evaluation and admission as evidence. The initial phase of the process, acquisition, indicates that a forensic investigator must first acquire digital evidence. The forensic investigator must possess the legal and technical ability to acquire digital evidence since acquisition is seen by Pollitt as both a legal and technical problem (Pollitt 1995, p.489). It is a legal problem since any acquisition of digital evidence must be within the ambit of the law for the evidence to be valid in court proceedings (Pollitt 1995, p.489). It is a technical problem

because the forensic investigator must possess the technical means and technical knowledge to acquire the evidence (Pollitt 1995, p.489).

Figure 3 – Pollitt's Computer Forensic Process from Pollitt (1995, p.3)

Pollitt considers the second phase, identification, or the identification of digital evidence, to consist of three steps. Digital evidence must first be "definable in its physical form" (Pollitt 1995, p.489). This means that the media upon which the evidence resides must be defined, for example, a CD or hard drive. The second step in identifying digital evidence is to identify the evidence's logical position on the physical media – that is, its place in the file system (Pollitt 1995, p.489). Finally, the evidence must be placed in the correct context so that its meaning may be ascertained. This can involve reading the evidence using an appropriate application (Pollitt 1995, p.489).

The evaluation phase follows the identification phase. In the evaluation phase, digital evidence is evaluated both technically and legally. Technical evaluations may determine who created the digital evidence, when and by what means (Pollitt 1995, p.490). Legal evaluations attempt to determine whether the digital evidence is relevant, reliable and if anyone can testify to it (Pollitt 1995, p.490).

Digital evidence that has been evaluated to be of a sufficient standard, both technically and legally, is then ready for the fourth and final phase where it can be admitted to court

as evidence. The name of the fourth phase is thus self-explanatory, namely: admission as evidence.

As mentioned earlier, Pollitt also defines terminology to describe digital evidence at the various phases of the investigative process. In the initial or acquisition phase, Pollitt describes digital evidence as media. After performing the three steps in the identification phase, the digital evidence is considered by Pollitt to be 'data'. The evaluations performed in the evaluation phase place the data in context, at which point Pollitt refers to the data as 'information'. Appropriate information is then presented as evidence. Figure 4 illustrates the aforementioned transitions graphically.

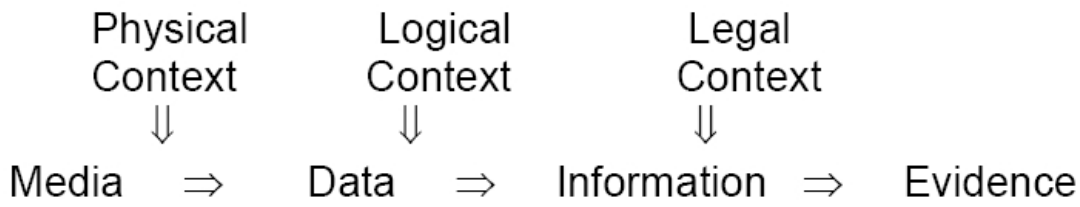

Figure 4 – Path taken by digital evidence from Pollitt (1995, p.4)

Next, we look at another prominent model by Beebe and Clark (2004).

3.2.1.2 Beebe and Clark's Framework

Beebe and Clark's Framework (Beebe & Clark 2004) is often cited in the DF literature, for example, by Pollitt (2007, p.7), Perumal (2009, p.39) and Ieong (2006, p.36). Beebe and Clark reviewed the literature on the DF investigation process and noted that the processes they found consisted of single tiers, whereas they posited that the DF investigation process involves multiple tiers (Pollitt 2007, p.7). Consequently, they put forward a hierarchical framework of the DF investigation processes that consisted of multiple tiers. At the highest level, or first tier of the framework, Beebe and Clark attempted to incorporate all the prevailing models of the time into their framework (Beebe & Clarke 2004, p.3). The phases in the first tier consisted of: preparation, incident response, data collection, data analysis, presentation of findings, and incident

closure. These phases are the high-level objectives that must be met in the sub-phases. The objectives of each phase are described briefly in the bullet list that follows.

- **Preparation phase:** In the preparation phase organisations optimise their response to an incident. That is, they attempt to take measures before an incident that maximises the availability and quality of digital evidence should such an incident occur (Beebe & Clarke 2004, p.3). Beebe and Clarke include activities such as: risk assessments; the development of incident response plans; training personnel; and preparing computing devices, amongst others.
- **Incident response phase:** In this phase suspected incidents are detected, reported, validated, assessed and a response strategy developed if needed. Beebe and Clarke (2004, p.4) point out that the response strategy should be a coordinated effort amongst "managerial, human, legal, and law enforcement resources". An initial plan for a DF investigation of the suspected incident should also be formulated in this phase.
- **Data collection phase:** The data collection phase starts once a decision has been made to initiate a digital investigation. The function of this phase is to collect digital evidence per the incident response and investigative plans. Beebe and Clarke (2004, p.4) note that some digital evidence is collected in the previous phase in order to validate an incident and determine its impact. It is the decision, however, to initiate a digital investigation that distinguishes data collection in the two phases. Some activities included in this phase are: obtain network-based and host-based evidence; ensure integrity and authenticity of digital evidence; and package, transport and store digital evidence (Beebe & Clarke 2004, p.4).
- **Data analysis phase:** Beebe and Clarke (2004, p.4) consider this phase "the most complex and time consuming phase in the digital investigations process". Analysis is performed in this phase to determine the truth of alleged suspicious activity and/or to reconstruct events. Such analysis is performed on data collected in the previous phase. Analysis activities include, but are not limited to: transformation of large amounts of data into sizes suitable for analysis; survey data to identify obvious digital evidence; and use data extraction techniques.

- **Presentation of findings phase:** In this phase findings from the analysis in the previous phase are communicated to all relevant people within the organisation. Beebe and Clarke (2004, p.5) specifically mention management, technical personnel, legal personnel and law enforcement as audiences findings can be communicated to. Findings may be presented orally or in a written format.
- **Incident closure phase:** The incident closure phase consists of four steps. The first step involves a critical review of the DF investigation process to "identify and apply lessons learned" (Beebe & Clarke 2004, p.5). The second step requires that decisions are made based on the results presented in the previous phase, and that such decisions are executed. In the third step, evidence is disposed of. Disposal should be with respect to legal requirements that may require retention rather than disposal of certain evidence. The final step in this phase requires that all information related to the incident be preserved.

The second and subsequent tiers of Beebe and Clarke's framework are intended to provide greater detail than is available in single-tier models (Beebe & Clarke 2004, p.6). Beebe and Clarke (2004, p.6) note that a number of authors of single-tier models suggest a need for greater detail in additional tiers. The purpose of including greater detail in the additional tiers is to capture the complexity of the DF investigative process. The additional tiers in Beebe and Clarke's model are termed objectives-based sub-phases (OBSP). Each lower level tier contains sub-phases of the phases contained in the tier above. The sub-phases in each tier contain objectives that must be met to satisfy the objectives of the phases in the tier above. Sub-phases themselves can contain tasks that must be executed to meet objectives of the sub-phases themselves. Figure 5 illustrates Beebe and Clarke's framework.

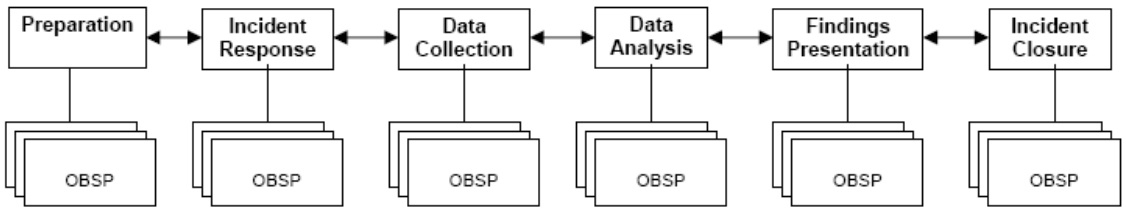

Figure 5 – Phases and objectives-based sub-phases (OBSP) in Beebe and Clarke's framework, from Beebe and Clarke (2004, p.8)

An example of sub-phases is provided by Beebe and Clarke (2004, p.10). They show how the use of the survey, extract and examine data analytic approach, known as the SEE approach, can be used to satisfy the objectives of the data analysis phase. The SEE approach requires that a digital object is first 'surveyed' for relevant data. The data is then extracted, and finally examined (Beebe & Clarke 2004, p.10). Each of these steps can be considered sub-phases of the overall data-analysis phase. The objectives of each of these sub-phases must be met in order to satisfy the overall objective of the data analysis phase. The relationship between sub-phases in the SEE approach and the data analysis phase can be seen in Figure 6. An example of a sub-phase objective is the 'Survey' sub-phase shown in Figure 6. In this sub-phase, the objective is to survey all possible sources of data for potential evidence.

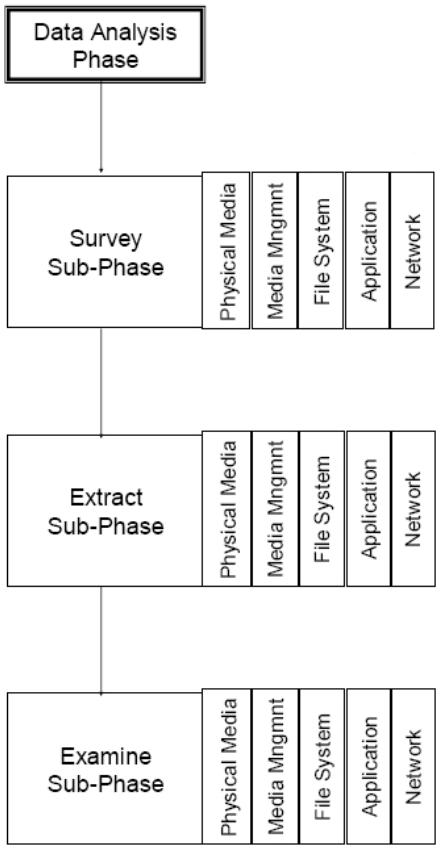

Figure 6 – The SEE data analytic approach and the data analysis phase, adapted from Beebe and Clarke (2004, p.11)

Beebe and Clarke (2004, p.9) state that to "the maximum extent possible, first-tier phases should be sequential and non-iterative". This does not mean, however, that an iterative

approach cannot be applied to first-tier phases when needed. They further state that experience in digital investigations suggest that sub-phases should be performed in an iterative manner. This is because the discovery of evidence, say in a sub-phase, may require another iteration of the sub-phases to search for new evidence. For example, in Figure 6, when evidence is extracted from a file system in the 'Survey' sub-phase, and examined in the 'Examine' sub-phase, the result of the examination may reveal that evidence could be found on physical media, which will require another iteration of the 'Survey', 'Extract' and 'Examine' sub-phases.

The last model we review is by Carrier and Spafford (2003, 2004). It is presented in the following section.

3.2.1.3 Carrier and Spafford's Framework

Carrier and Spafford (2003, 2004) put forward a framework for the DF investigative process that is modelled on the forensic investigative process for physical crime scenes. At the heart of the framework is a digital investigation process model consisting of seventeen phases that are organized into five groups. These groups are: readiness, deployment, physical crime scene investigation, digital crime scene investigation and presentation. In this section we discuss each of the groups briefly.

- **Readiness phases:** The readiness phases exist to ensure that an organisation is adequately prepared to conduct an investigation when the need arises. Two readiness phases are described in Carrier and Spafford's process model, namely an operations readiness phase and an infrastructure readiness phase. The operations readiness phase focuses on making sure that the relevant personnel are sufficiently trained prior to an investigation. The relevant people are considered by Carrier and Spafford to include staff who will read DF reports as well as those who will conduct the DF investigation. Equipment used by investigators must also be maintained as part of the operations readiness phase. The infrastructure readiness phase is concerned with configuring infrastructure in such a way that it supports an investigation. For example, ensuring logging is active on networking equipment and network hosts. The readiness phase is not related to a particular incident and occurs continuously.
- **Deployment phases:** The purpose of the deployment phases "is to provide a mechanism for the incident to be detected and confirmed" (Carrier & Spafford

2003, p.7). There are two deployment phases: (1) the detection and notification (DN) phase, and (2) the confirmation and authorisation (CA) phase. The DN phase, as its name suggests, marks the point at which the incident is detected and the organisation made aware of the incident. The CA phase is also self-explanatory – authorisation to conduct a full investigation is obtained in this phase. Such authorisation needs to be valid both from a legal and organisational policy perspective.

- **Physical crime scene investigation phases:** The physical crime scene phases focus on examining physical objects in the vicinity of the digital device of interest. Physical objects are examined with the intention of reconstructing events, or providing links between individuals and digital events. For example, a fingerprint on a keyboard may establish the physical presence of a suspect at a computer. Carrier and Spafford consider digital devices to be physical objects and the data contained within these to be digital data. Thus, securing or processing the physical crime scene also involves securing or processing digital devices at the crime scene. Where digital devices are suspected of being used in the crime or incident, the examination of the digital data contained on the devices marks the beginning of the digital crime scene investigation phases. The physical crime scene phases included in the model are not novel contributions by Carrier and Spafford but rather the standard phases in physical crime scene investigation (Carrier & Spafford 2003, p.8).
- **Digital crime scene investigation phases:** The primary function of the digital crime scene investigation (DCSI) phases is to examine the digital data on digital devices. The model dictates that an investigation is undertaken for each self-contained digital device (Carrier & Spafford 2004, p.5). Six phases make up the DCSI phases, they are the: preservation, survey, documentation, search and collection, reconstruction, and presentation phases. In the preservation phase digital data is preserved to ensure it is in the same state as it was found in. The survey phase involves a broad examination of the digital data for obvious digital evidence. Each individual piece of evidence found in the survey phase is documented in the documentation phase. A more thorough analysis of the digital

data is performed in the search and collection phase, the aim of which is to find further digital evidence. Knowledge gained from the survey phase is used when conducting the search and collection phase. In the reconstruction phase the incident is reconstructed based on theories on how the incident occurred. These theories are developed from the evidence. In the presentation phase investigation findings are shared amongst investigation teams if more than one team is involved. The findings are then integrated.

- **Review phases:** The review phases involve a post-mortem or performance review of the investigation process. Areas for improvement are identified here to ensure any mistakes are not carried forward into future investigations.

Figure 7 below shows the five groups of phases in Carrier and Spafford's framework.

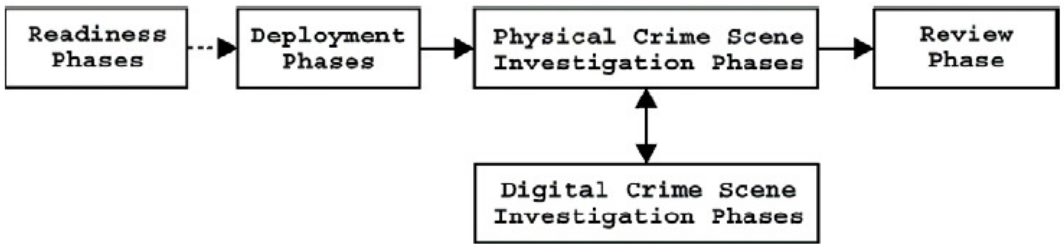

Figure 7 – Carrier and Spafford's process model for DF, from Carrier and Spafford (2003, p.7)

In the discussion on digital forensic readiness that follows, and in this thesis in general, we use Carrier and Spafford's process model since it explicitly recognises digital forensic readiness as part of the DF process.

3.3 Conclusion

In this chapter we examined the field of digital forensics (DF) and presented a selection of the many definitions of DF. We also put forward the definition we use for this thesis, which we adapt from Kruse & Heiser (2001, p.1) and Palmer (2001, p.17). We define DF as the scientific discipline that concerns itself with the preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary or root cause analysis, or the anticipation of unauthorised actions that may be disruptive to planned operations. Differing terminology also exists in the field of DF, hence we

differentiated the terms ‘digital forensics’ and ‘computer forensics’. We also defined terms such as ‘digital objects’ and ‘digital data’ for later use.

To illustrate the digital forensic investigation process, we presented the prominent models from the following authors: Pollitt (1995), Beebe and Clarke (2004) and Carrier and Spafford (2003, 2004). Carrier and Spafford’s model was chosen as the model that will be used for the thesis because it explicitly recognises digital forensic readiness.

The next chapter addresses digital forensic readiness.

4 Digital Forensics Readiness

4.1 Introduction

Digital forensic readiness (DFR) is a relatively new concept and little has been written on the topic in contrast to the field of DF as a whole. Our review of the literature on DF shows the first work on the topic by Tan (2001). Since then, authors have focused on the technical aspects of DFR and, to a lesser degree, on the non-technical and organisational aspects. In this section we further explain DFR. We place more emphasis on the organisational aspects of DFR since this thesis is more concerned with DFR from an organisational perspective.

Tan first defined DFR as the pursuit of two objectives, namely: (1) maximising an environment's ability to collect credible digital evidence, and; (2) minimising the cost of forensics during an incident response (Tan 2001, p.1). This definition of DFR is commonly used in the literature (Rowlingson 2004)(Danielsson & Tjøstheim 2004)(Endicott-Popovsky et al. 2007); however, for this thesis we use the definition by Rowlingson (2004, p.5) that is based on Tan's definition. Rowlingson defines DFR as:

Those actions, technical and non-technical, that maximise an organisation's ability to use digital evidence whilst minimising the costs of an investigation.

Rowlingson's definition specifically mentions organisations, which is more suited to this thesis. Furthermore, by using an organisational context Rowlingson is able to make the distinction between technical and non-technical actions, which Tan does not, since Tan's work was predominantly technical.

In our discussion of DFR that follows, we look at contributions to DFR that take organisational context into consideration. A number of purely technical problems exist within DFR in which organisational context is not relevant. For example, research by Seifert et al. (2008) on the need for forensically ready network protocols. Another example is Ngobeni and Venter's model for forensic readiness in wireless networks (Ngobeni & Venter 2009). We do not discuss the purely technical contributions as they

are outside the scope of this work. The remainder of this chapter contains the following section on the organisational aspects of DFR and the conclusion.

4.2 Organisational Aspects of Digital Forensic Readiness

In this section we review the DFR literature in chronological order. Tan's seminal contribution is first discussed, followed by Yasinsac and Manzano, and then Wolfe and Wolfe-Wilson. The major contribution by Rowlingson is then presented after which Danielsson and Tjøstheim is discussed. A review of Casey and Endicott-Popovsky et al. follows, and finally the work of Grobler et al. and Pangalos et al is addressed.

4.2.1 Early Identification of Technical Factors

The earliest work exclusively on DFR, as mentioned previously, was proposed by Tan (2001). Besides defining DFR, Tan provides insight into the organisational and technical requirements of DFR. He identifies incident data as being of importance in DFR and lists four possible sources of incident data (Tan 2001, p.2):

1. The victim system(s) RAM, registers and raw disk.
2. The attacking system(s) RAM, registers and raw disk.
3. Logs (from the victim and attacking systems as well as intermediary systems).
4. Physical security at the attacking system (e.g., camera monitoring, etc.).

Tan states that the cost of an incident is proportionate to the amount of time taken to investigate it. The implication is thus that preparedness for an incident reduces the time taken to investigate it and in turn reduces the cost of an investigation. The primary contribution of Tan in his seminal work, however, is his identification of five elements of DFR (Tan 2001). These elements are important since they affect "evidence preservation and time to execute" (Tan 2001, p.3). They are:

- **How Logging is Done.** In order to facilitate the acquisition of incident data, Tan advocates multi-tier logging. Multi-tier logging entails logging at multiple points in a network and at different levels in network hosts. An example of logging at multiple points in a network is to enable logging on routers and switches residing on an internal network, and not simply enabling logging on network perimeter

devices such as firewalls. An example of logging at different levels in a network host is to enable application-level and operating system-level logging on a server. This allows for the validation of incident data by corroborating logs against each other. Tan also provides technical detail on enhancing the effectiveness of logging, by amongst others, mechanisms such as the use of a central logging server to store logs and a time server to synchronise time on logging devices. Logs should be retained as long as possible, keeping in mind the laws and policies related to data retention and the risk to the organisation itself by retaining data.

- **What is Logged.** Network hosts and network infrastructure should have logging enabled. Tan considers the logging of processes, file-systems, network and security events to be the most useful logging on host computers. Additionally, logging should be enabled on network devices such as firewalls, intrusion detection systems, domain name servers, routers, proxy and dial-up servers, amongst others.
- **Intrusion Detection Systems.** Tan recommends using both network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS) for the purposes of DFR. He also suggests correlating alarms from each type of intrusion detection system to narrow wide-scale searches in DF investigations.
- **Forensic Acquisition.** The acquisition of data from digital devices during a DF investigation should occur as soon as possible after notification of an incident. For this reason Tan suggests that efforts on DFR should concentrate on developing procedures and mechanisms to acquire and preserve incident-related data that should be defined prior to an incident occurring. Special attention should be given to systems that are complex as these may require different procedures than those used on common systems.
- **Evidence Handling.** Tan stresses the importance of the chain of custody of digital evidence. To this end, he notes that, as part of DFR efforts, a chain of custody document should exist to track the chain of custody of digital evidence. The chain of custody document should be readily available and detailed for recording physical & logical attributes of evidence. DFR measures should also ensure that the transport of evidence, whether physically, or over a network, is

secure. The same applies to the storage of evidence – DFR efforts should ensure that a secure storage capability exists in advance of the need to store physical evidence, such as a device, or digital evidence, such as data.

It is important to note that Tan states explicitly that the five elements involve both "technical and non-technical factors" (Tan 2001, p.3). Tan, however, does not provide much detail on the non-technical factors.

4.2.2 Organisational Policy and Early Non-technical Aspects

Yasinsac and Manzano (2001, p.290-1), writing at a similar time to Tan, do provide a little further detail regarding non-technical factors. They note that organisational policy should form the basis for evidence acquisition and retention. Moreover, they address aspects such as the composition of the forensics team and DF training requirements. They suggest that an organisation's forensics team should be multi-disciplinary and include staff from senior management, the human resources and IT departments, as well as external help, such as consultants. Training for the incident response team, investigative team and all computer users in the organisation is also suggested by Yasinsac and Manzano (2001, p.292-3). Wolfe and Wolfe-Wilson (2003, p.61) consider the importance of managing internal and external communications in the event of an incident. They advise using a central point of communication to ensure the information released is accurate and does not hamper the investigation or harm the organisation in other ways.

4.2.3 A Comprehensive Approach

Rowlingson (2004, 2005) presents a ten step process for attaining DFR. It is the most detailed work on the organisational aspects of DFR in the literature at the time of writing. It also concentrates more on non-technical factors. Rowlingson's ten steps are intended as practical means by which to implement DFR measures in an organisation (Rowlingson 2004, p.8). The ten steps are:

1. Define the business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.

3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

We elaborate on each of these steps in the discussion that follows.

- **Define the business scenarios that require digital evidence**. The first step that Rowlingson requires is a risk assessment. The organisation should determine the scenarios in which it is most at risk and which have the greatest impact. The scenarios in which digital evidence provides the most benefit with respect to risk and impact should be chosen. Amongst others, Rowlingson notes that, digital evidence can be used to: reduce the impact of computer-related crime; help deal with court-orders to release data; demonstrate legal or regulatory compliance; support disciplinary action against staff; prove the impact of a crime or dispute (Rowlingson 2005, p.6). Where the risk assessment shows that DFR measures are sufficiently beneficial, the next step involves determining the specific evidence to collect.
- **Identify available sources and different types of potential evidence.** Before determining the specific evidence to collect, it is necessary to identify all the sources and types of digital evidence in a particular scenario. Rowlingson (2004, 2005) provides an exhaustive list of digital devices and software that can be useful sources of information. In essence, all digital devices and all software capable of generating digital evidence should be considered. This corresponds with the second element of Tan's five elements of DFR presented earlier.

Rowlingson, however, goes further in that he puts forward questions that are important from organisational and non-technical point of view. For example, who is responsible for specific data? Who is the formal owner of the data? Such questions are important since, in the event of an incident, staff may not release data without the appropriate manager's or director's permission. As mentioned earlier, Tan (2001) points out that data acquisition should occur as soon after an incident as possible. Attempting to determine data owners post-incident may result in a significant delay.

- **Determine the evidence collection requirement.** In this step, the organisation evaluates which of the evidence sources and types identified in the previous step it will use. There will be a cost associated with collecting each source and type of evidence – for example, it may be necessary to purchase certain tools to extract or store certain types of evidence. Rowlingson states that the evaluation of the evidence collection requirement should be subject to a cost-benefit analysis. An important outcome of this step is an evidence requirement statement. An evidence requirement statement serves as an agreement between those responsible for DF and those responsible for "running and monitoring information systems" (Rowlingson 2005, p.7). The statement is important as it lays out clearly the evidence collection responsibilities of the operations and monitoring staff.
- **Establish a capability for securely gathering legally admissible evidence to meet the requirement.** Once the evidence collection requirement has been determined, the next step is to ensure that the evidence is collected and preserved in an appropriate manner. That is, the collection should be done in a manner which conforms to the law. Rowlingson specifically states that legal advice is required at this stage (Rowlingson 2005, p.8). The need for secure evidence storage is also noted by Rowlingson. This corresponds to recommendations by Tan in his evidence handling principle of DFR that was mentioned earlier.
- **Establish a policy for secure storage and handling of potential evidence.** The secure evidence storage referred to by Rowlingson in this step refers to long-term or off-line storage for evidence that may be required in the future. The key outcome of this step is a secure evidence policy that provides guidance on how

evidence should be securely stored and handled in order to maintain the chain of custody. Chain of custody refers to the recording of "who held, and who had access to, the evidence" (Rowlingson 2005, p.8). The importance of policy in this regard is in line with Yasinsac and Manzano (2001) mentioned earlier.

- **Ensure monitoring is targeted to detect and deter major incidents.** Rowlingson advocates a 'suspicion' policy as a product of this step. This is a document that helps monitoring and auditing staff determine what suspicious behaviour or events to look for when performing their duties. Rowlingson believes that evidence sources should be monitored to detect potential threats or incidents in advance. It is important to note that Rowlingson's inclusion of the active monitoring of evidence as part of DFR, implies that DFR is not simply *a priori* preparation in anticipation of an incident, but also a means to prevent an incident from occurring.
- **Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.** Suspicious events detected in the previous step need to be reviewed to determine if they warrant further investigation. Rowlingson recommends that an escalation policy be used to provide guidance on the escalation process. The policy should state who should be contacted depending on the type of suspicious behaviour detected. As with previous steps, the policy also serves to inform management from different organisational functions what their responsibilities are during the escalation process and how they should interact with each other. Rowlingson states that the decision on whether escalation should occur should be based on the potential impact of the suspicious behaviour and if a "full investigation may be required where digital evidence may be needed" (Rowlingson 2005, p.10). In order to evaluate the impact Rowlingson advocates a preliminary business impact assessment. He provides detailed criteria that can be used in such an impact assessment (Rowlingson 2005, p.10).
- **Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.** Rowlingson points out that it is important for staff to understand their role not

only during incident response, but also before and during an incident. He suggests that information be divulged only on a 'need-to-know' basis and that 'whistle blowers' names be kept confidential and that they be offered protection from retaliation. Specialised training is recommended for, amongst others, those involved in the following corporate functions: investigating team; corporate human resources; corporate public relations; 'owners' of business processes or data; line management and profit centre managers; corporate security; IT management and system administrators; legal advisors.

- **Document an evidence-based case describing the incident and its impact.** Investigations should not be limited to identifying a perpetrator and repairing any damage caused by the perpetrator. Rowlingson states that an investigation must provide answers to questions such as who, what, why, when, where and how. Moreover, the investigation should be able to show why the answers it provides are credible through appropriate evidence and a logical argument. Again, Rowlingson advocates policy as a means of providing guidance. In this instance, a policy that guides the creation of an evidence-based case should be developed. An evidence based case has the advantage of being useful in, for example, support of an insurance claim or regulatory reporting.
- **Ensure legal review to facilitate action in response to the incident.** Rowlingson notes the necessity of obtaining legal opinion at certain points in building a case and once the case has been built. Legal advice is necessary in order to determine if the case is strong enough for its intended purpose, for example, a disciplinary action. Legal advisors need to be properly trained and experienced in the law as it applies to digital evidence collection and use. Further, they should be aware of the legal implications where multiple legal jurisdictions are involved. Legal advisors also need to be consulted in order to help an organisation determine when and if law enforcement should be contacted.

Rowlingson's ten steps provide a broad and comprehensive outline of DFR. The ten steps show that the scope of DFR is not limited to the technical requirements for evidence collection. Rather, the effort to develop and maintain a DFR capability within an organisation is an organisation-wide effort involving multiple functional areas within the

organisation. We believe Rowlingson's first step is of critical importance within an organisation. It forces organisations to look at the business scenarios that are most at risk and which benefit most from DFR. This is important because it encourages organisations to take an organised approach to DFR rather than an ad-hoc approach. In focussing on high-risk business scenarios we believe organisations are most likely to apply DFR measures to the areas that hold the best return on their investment in DFR. Contributions to the DFR literature subsequent to Rowlingson's ten steps have not been as comprehensive.

4.2.4 Law Enforcement and Information Privacy Sensitive Forensics

Danielsson and Tjøstheim (2004), who wrote not long after Rowlingson, note that in many areas the law does not clearly delineate the responsibility between organisations and law enforcement with regard to crimes or incidents that may require a DF response (Danielsson & Tjøstheim 2004, p.419). They point out that, in any event, an organisation that collects and preserves digital evidence in an appropriate manner, increases the ability of law enforcement to collect such data. Danielsson and Tjøstheim (2004, p.419-420) also raise the issue of the tension between DF on the one hand, and the privacy of an organisations staff and data subjects, on the other hand – DF seeks to record user actions and data, while privacy seeks to limit access to the same. They provide two suggestions in this regard. First, that privacy enhancing technologies be incorporated into DFR tools and components, and second that DFR implementations take cognisance of privacy-related legislation (Danielsson & Tjøstheim 2004, p.419-420).

4.2.5 Importance of Training, Per Incident Costs, Network Forensic Readiness and Strategy

Casey (2005) reinforces some of Rowlingson's points on DFR through practical lessons learned in a case study. In particular Casey highlights the importance of training system administrators and incident handlers on the correct way to respond to an incident (Casey 2005, p.259). Casey (2005, p.259) also notes how the secure storage of potential evidence helped the investigation carried out in his case study. Lastly, Casey's case study indicates that DFR "reduces the per incident costs" (Casey 2005, p.259).

Endicott-Popovsky et al. (2007) discuss network forensic readiness (NFR) and the lack of a single, comprehensive organisation-wide framework that facilitates the implementation of NFR (Endicott-Popovsky et al. 2007, p.1,4). They propose an organisation-wide framework to ensure NFR in an organisation. They argue that DF has a function in all the aspects of information assurance, where information assurance is defined as: "Information operations (IO) that protect and defend information and information systems ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities" (Maconachy et al. 2001, p.306). As such, Endicott-Popovsky et al. (2007, p.5-6) state that for a network to be forensically ready, NFR must take into consideration security policies, procedures, practices, mechanisms, and security awareness training programs. This is in agreement with what is contained in Rowlingson's ten steps.

Endicott-Popovsky et al. (2007, p.6) also put forward a strategy model to assist in the development of organisational policy regarding information assurance and DFR. The model is known as the 4R Model for Strategies for Accountable Systems (4R Model). In the model, the four strategies of resistance, recognition, recovery and redress are used to ensure an adequate level of security and accountability for those that breach security. The 4R Model is summarised in Figure 8.

Strategy	Tools
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react / adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • ("forensics" - *the what)* • Replication • Backup systems • Fault tolerant designs
Redress 1) Ability to hold intruders accountable in a court of law. 2) Ability to retaliate	• Forensics - *the who* • Legal remedies • Active defense

Figure 8 – 4R Model for Strategies for Accountable Systems, from Endicott-Popovsky et al. (2007, p.6)

The 4R Model is applied to the NIST Information Systems Development Life Cycle (ISDLC) (Kissel et al. 2008) by Endicott-Popovsky et al. to develop an implementation methodology for NFR. The methodology is called the Network Forensics Development Life Cycle (NFDLC). The DFR procedures that have been added to the ISDLC to form the NFDLC are shown in Figure 9 below.

ISDLC Phases	NFDLC Additional Procedures
Initiation Phase: preliminary risk assessment	Determine what aspects of a network would warrant digital forensic protection
Acquisition/Development Phase	Adhere to Rules of Evidence in system requirements Apply published forensic checklists
Implementation Phase	Perform baseline testing Perform network/mechanism verification/calibration tests
Operation/Maintenance Phase	Conduct verification/calibration audits
Disposition Phase	Incorporate chain of custody/evidence preservation procedures

Figure 9 – DFR procedures in the NFDLC, adapted from Endicott-Popovsky et al. (2007, p.7)

Endicott-Popovsky et al. discuss NFR, which is a more specific form of DFR. Although this is the case, we believe that the strategies and models they put forward can be generalised to DFR as a whole.

4.2.6 Incorporating Digital Forensics into Other Corporate Functions

Grobler et al. (2010, p.647) note the need for "a comprehensive DF Management Framework (DFMF)" and propose a high-level framework to that end. A component of their framework covers what they call Proactive DF. Proactive DF is essentially DFR; however, they link DFR with corporate governance and define Proactive DF as "the proactive restructuring and defining of processes, procedures and technologies to create, collect, preserve and manage [digital evidence] to facilitate a successful, cost effective

investigation, with minimal disruption of business activities whilst demonstrating good corporate governance". They note that DF tools can be used to assess information security controls and that following the DF investigation process provides documented proof of the assessment, which enhances corporate governance. We do not agree with Grobler et al. in this respect for the following reason. In essence, they propose the use of DF tools to perform testing of security controls. This is usually part of the audit function of an organisation. We believe that using DF tools that are available as a result of DFR, in order to perform an audit function, should not expand the definition of DFR to include auditing. The access to DF tools is rather an added benefit to audit, not something that is sufficiently inherent in DFR that it merits being part of the definition of DFR.

While Endicott-Popovsky et al. (2007, p.5-6) require that NFR takes security policies into consideration, Pangalos et al. (2010) make the case for DFR in general. Pangalos et al. (2010, p.15-16) endorse the 4R Model and state that security policies should be assessed with DFR in mind. Pangalos et al. (2010, p.15) also make a more convincing argument than Grobler et al. that DFR enhances corporate governance. They argue that corporate governance requires management in an organisation to take responsibility for the "security health" of IT systems. The implementation and use of DFR shows that management is prepared to deal with incidents appropriately should they occur. Pangalos et al. (2010, p.16) also note the need for dedicated forensic roles within an organisation. They anticipate that as the stature of DF increases, dedicated DF roles will emerge similar to the existing Chief Information Security Officer role.

In the following section we summarise and conclude this chapter.

4.3 Conclusion

In this chapter we examined digital forensic readiness (DFR). DFR is a field within the larger field of digital forensics (DF). In our review of DFR we presented the definition of DFR by Tan (2001); however, we adopted the definition by Rowlingson (2001, p.4-5) since it takes organisational context into account. Rowlingson defines DFR as those actions, technical and non-technical, that maximise an organisation's ability to use digital evidence whilst minimising the costs of an investigation.

Our review of DFR did not include purely technical contributions to the field, but rather focused on the organisational aspects of DFR. Accordingly, we presented a review of the literature on the organisational aspects of DFR. The review was presented in chronological order and highlighted contributions made by each author. A summary of the authors reviewed in chronological order can be seen in Figure 10 below. Where authors repeated the conclusions or points of previous contributors, we did not include this in our review. Seminal contributions were made by Tan (2001) and Rowlingson (2001), with Rowlingson providing the most comprehensive treatment of DFR in organisations. The fundamentals laid down by these two authors have largely been echoed in subsequent work, with other authors making relatively small contributions. An exception to this trend is the work by Endicott-Popovsky et al. (2007) on the narrower field of network forensic readiness (NFR). They put forward a methodology to develop policies that take NFR into account. They also develop an implementation methodology for NFR. Both of these methodologies can conceivably be applied to DFR in general without significant effort.

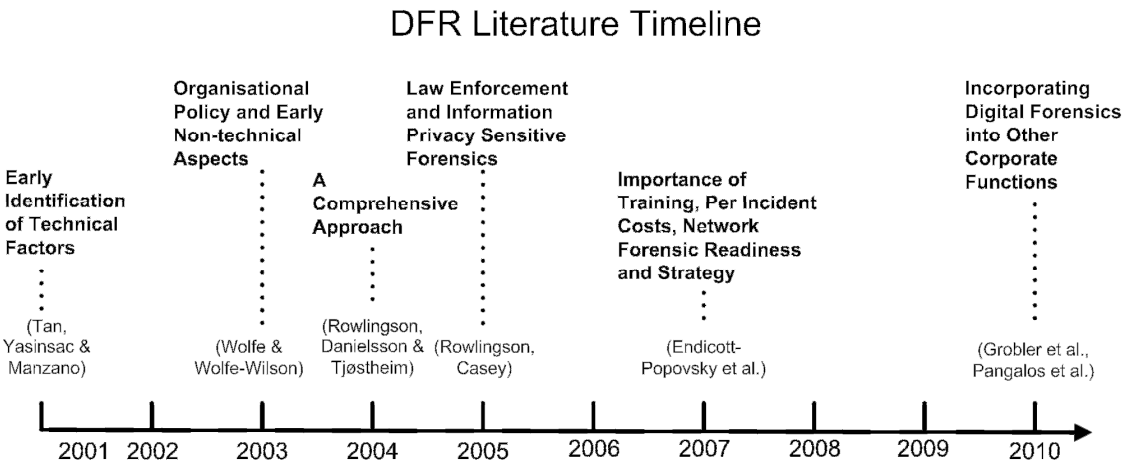

Figure 10 – Timeline of explicit DFR contributions reviewed in this chapter.

This chapter provided the definition of DFR that will be used in the remainder of the thesis. It also provided background on the organisational aspects of DFR that are necessary to understand the contributions made later in Part 2 of the thesis.

In the next chapter we depart the discipline of digital forensics and discuss Time-Driven Activity-Based Costing (TDABC), a method used to determine cost in organisations.

TDABC is discussed since it is used in the chapters in Part 2 that focus on determining the cost of DFR-related activities.

5 Time-Driven Activity-Based Costing

5.1 Introduction

Management accounting is the field of accounting "concerned with providing information to managers for use in planning and controlling operations and in decision making" (Garrison et al. 2006, p.4). Within management accounting, the techniques used to allocate costs in an organisation are known as cost systems. Traditional cost systems are not adept at providing cost information for specific activities (Brimson 1991, p.7-11)(Gunasekaran 1999, p.118-9). This makes it difficult for management in an organisation to make cost-related decisions about activities within the organisation. Alternative cost systems, however, can often provide better insights to management. Each of these alternative cost systems offers different advantages over traditional costing and over each other (Gurowka & Lawson, 2007). We focus on Time-Driven Activity-Based Costing (TDABC), which is a cost system that is used to determine, or estimate, the cost of specific activities. TDABC is derived from an earlier cost system known as Activity-Based Costing (ABC). ABC and TDABC may provide management with the information it needs to understand and optimise resource usage and costs within the various activities in an organisation (Ooi & Soh 2003, p.55). With the exception of Resource Consumption Accounting (RCA), no other alternative costing system provides management with detailed cost information about activities. While it is conceptually possible to track the costs of activities using RCA it is difficult as activities are not the implicit unit of analysis for resource consumption (Balakrishnan et al. 2012, p.33). It is for this reason that we choose TDABC.

In this chapter we first discuss Activity-Based Costing (ABC) since it is the basis from which TDABC was derived. The terminology, concepts and definitions introduced in the discussion of ABC are also used in the section on TDABC that follows. The section on TDABC includes an example of how TDABC is used to calculate the cost of an activity.

At the time of writing this thesis, the content of this chapter was accepted for publication in the journal Information Systems Frontiers (Reddy et al. 2011) and published "online first". No further information on which volume and issue the article would be published

in was provided by the journal, therefore the citation is to the Digital Object Identifier (DOI) provided by the journal.

5.2 Activity Based Costing

ABC arose out of the inability of traditional cost systems to provide accurate information in modern business organisations, which had changed significantly from the older businesses that traditional cost systems were designed to cater for (Brimson 1991, p.7-11). In particular, Gunasekaran (1999, p.118-120) states that traditional cost systems do not: report the costs of particular activities performed in the business; accurately reflect the cost of different types of products or services when there is a large diversity of products or services; encourage improvements in the business; and lastly, do not adequately take the increased cost of overheads in modern businesses, such as marketing and IT, into account.

Activities can be defined as the aggregation of tasks, performed by people or machines, to produce a given product or service (Brimson 1991, p.46)(Gunasekaran 1999, p.118-120). In ABC activities are said to consume, or use, resources. Products or services, in turn, consume activities. To implement ABC, it is therefore necessary to trace the cost of all the resources used by an activity to determine what is known as the activity cost of that activity. Activity costs are then traced to cost objectives (products or services), based on the activities used to create the cost objective – this yields the cost of the cost objective. In traditional cost systems, cost objectives consume resources directly, making it difficult or impossible to accurately derive activity-specific information.

ABC is widely considered to consist of the following basic phases, though other expositions may combine some of these phases (the phases that make up TDABC, on the other hand, can be seen in the next section):

1. Identify activities: In this phase all the significant activities undertaken by the business are identified. All of these activities are recorded in an activity directory. Each variation of an activity is recorded as a separate activity in the activity directory. Surveys or interviews of employees are also usually carried out to determine the extent of employees' involvement in the various activities.

2. Trace resource costs to activities: During this step the resources used by an activity are traced to the activity. As mentioned, the cost of the resources that are used by an activity is termed the activity cost of that activity. Activity costs can be grouped together to form activity cost pools.

3. Determine cost drivers: Cost drivers measure the frequency and intensity of the demands placed on activities by products or services (Ooi & Soh 2003). In this phase cost drivers are defined for each activity. For example, consider an activity in which orders are processed – the more orders that are processed in a given time period, the higher the cost of order processing for the particular product or service. The cost driver for this activity, namely order processing, is the number of orders. The reason is that the cost of the activity is most strongly correlated with the number of orders. Cost drivers allow the activity cost to be stated in terms of a rate, such as dollars per order processed, which is known as a cost driver rate. Cost driver rates allow management to evaluate performance.

4. Assign activity costs to cost objectives: In this step the costs are assigned to the cost objective by multiplying the actual volume of cost driver units (e.g. orders) by the cost driver rate.

5.3 Time-Driven Activity-Based Costing

Time-Driven Activity-Based Costing (TDABC) (Kaplan & Anderson 2004; 2007a; 2007b), like ABC, is also a cost system. It was developed to help overcome some of the problems with ABC that resulted in failures of ABC implementations and a relatively low uptake of ABC by businesses (Gosselin 2007)(Kaplan & Anderson 2007b, p.5-7)(Malmi 1997). Implementations and tests of TDABC have shown it to be simpler, cheaper, and more powerful than ABC (Kaplan & Anderson 2007b).

TDABC overcomes some of these problems by employing a simpler process to derive cost information for activities. It uses time-equations to assign the cost of resources (Kaplan & Anderson 2007a, p.5-15). We discuss the TDABC process next.

5.3.1 The TDABC Process

The TDABC process consists of the following steps:

1. Identify activities: In this step the activities for which cost information is desired are identified.

2. Determine capacity cost rate: The capacity cost rate applicable to the activities must be calculated. Capacity cost rate can be defined by equation (1) below.

$$(1)\quad \text{Capacity cost rate} = \frac{\text{Cost of capacity supplied}}{\text{Practical capacity of resources supplied}}$$

The cost of the capacity supplied refers to the cost of the resources used to perform the activities. Typically this includes the cost of salaries for the employees performing the activity, equipment and technology costs, rental of office space and any other costs incurred (Kaplan and Anderson 2007b, p.41). Practical capacity is measured in units of time. It refers to the actual capacity of resources, rather than their theoretical maximum capacity. That is, the amount of time strictly dedicated to performing the activity, as opposed to the amount of time theoretically available for performing the activity. Kaplan and Anderson (2004, p.133), for example, suggest using a practical capacity of 80% to 85% for employees. This takes into account non-productive time spent by employees during a working day. The capacity cost rate is given as a ratio of units of currency per unit time.

3. Estimate activity time: Management estimates the amount of time it takes to complete a single unit of the activity in this step. A single unit of an activity means, for example, how long it takes an employee to complete a single order. Kaplan and Anderson (2007b, p.11) state that estimates which are accurate to within a few percentage points suffice while large errors will become clear through capacity excesses or shortfalls. They note that activity times are typically "stable for several periods" and that average or standard times are often reviewed annually. It should be noted, however, that such excesses or shortfalls may also be the result of a specific event that occurs during a period. In such instances, if the event is not immediately identified as the source of the excess or shortfall, further attempts may be required to determine a more accurate time.

Such attempts may involve different techniques, for example, direct observation, which can be used to validate an employee's estimate.

4. Determine cost driver rate: The cost driver rate for an activity in TDABC is simply the product of the capacity cost rate and the time estimate for a single unit of the activity. As an example, if the capacity cost rate for the activity of taking an order was determined as $2 / minute and it was estimated that an order took fifteen minutes to complete, the cost driver rate for taking an order would be $30. The product of capacity cost rate and time estimate represents the simplest form of time equation used in TDABC. Time equations are discussed in further detail in the example later in this section.

5. Assign activity costs to cost objectives: The costs are assigned to the cost objective by multiplying the actual volume of cost driver units by the cost driver rate.

Next, we illustrate the TDABC process by way of a simple example.

5.3.2 An Example of TDABC

The interceptions department of a hypothetical large cellular network operator in South Africa handles requests by law enforcement officials for voice, data and location information as part of its daily operations. The service provider must provide this information in response to legal requests by the law enforcement officials (Republic of South Africa 2002). Step 1 in the TDABC process requires that we define the activities for which cost information is desired. For the sake of simplicity in the example, we assume the interceptions department performs three activities, namely: evaluate request; process request; and lastly, provide feedback for warrantless intercept requests. The first two activities are self-explanatory; however, the third activity is a requirement of a South African law (Republic of South Africa 2002) that allows for intercepts without a judicial warrant, or warrantless intercepts, under certain circumstances. When warrantless intercepts are requested and the network operator performs the intercept, the operator is legally bound to provide a report to a judge about the intercept.

We assume the total monthly cost of resources, or cost of capacity supplied, for the interceptions department is R800 000 ('R' stands for 'Rand' which is the currency used

in South Africa). This cost includes salaries, equipment, office rental and other costs incurred by the department. The department employs ten individuals who each work eight hours, or 480 minutes, a day – the theoretical maximum capacity of all the workers in a month. Together all employees work 4800 minutes a day or 96000 minutes a month. To determine the practical capacity, we take 80% of this, which is 76800 minutes. We can now perform step 2 and calculate the capacity cost rate, which is the cost of capacity supplied divided by the practical capacity. In our example this is R800000 / 768000 minutes, which results in a capacity cost rate of R1.04 / minute.

In step 3 we must determine the activity time for the three activities. In our example, we assume these have been measured and found to average the following values:

- evaluate request – 31 minutes
- process request – 62 minutes
- warrantless intercept feedback – 82 minutes

Table 5 – Monthly departmental costs for interceptions department

Activity	Cost Driver Rate	Volume	Monthly Cost
evaluate request	R32.24	145	R4674.80
process request	R64.48	112	R7221.76
warrantless intercept feedback	R85.28	13	R1074.32
Total			**R12970.88**

The determination of cost driver rates for each activity is the final step in TDABC. The cost diver rate for each activity is the product of the department's capacity cost rate and activity time for each activity. For example, in the case of the 'evaluate request' activity, the activity time is 31 minutes and the capacity cost rate is R1.04 / minute. The cost driver rate for the activity is thus R32.24. This implies that it costs the network operator R32.24 to evaluate an interception request. Calculating the cost driver rate for the remaining two activities is done in the same way: the cost driver rate for the 'process request' activity is R64.48 and for the 'warrantless intercept feedback' activity, R85.28. Given the volumes of each activity, it is possible to calculate the monthly cost for each of

these activities using equation (2) below. The monthly costs and the total monthly cost are shown in Table 5.

(2) Total Activity Cost = Cost Driver Rate × Volume

In Table 5 we listed the time for each activity separately, in a similar fashion to traditional ABC. The times in the table can, in fact, be represented as a single equation known in TDABC as a time equation, which is shown in equation (3).

(3) Total time for intercepts department = 31 × (volume of requests evaluated) + 62 × (volume of requests processed) + 82 × (volume of warrantless intercept feedback given)

The total activity cost can then be calculated by multiplying the result of equation (3) by the capacity cost rate of the department, which is R1.04 / minute. When a single capacity cost rate is used, as in this example, the total cost can be given by equation (4).

(4) $\text{Total Activity Cost} = c\sum_{i=1}^{n} t_i v_i$, where c is the capacity cost rate, n the number of activities, t the time to complete the i^{th} activity, and v the volume of the i^{th} activity.

In the example thus far we have assumed that evaluating all types of requests takes the same amount of time. Time equations can also be used to capture variations in activities. Take the 'evaluate request' activity, for example. Evaluating an emergency request by a law enforcement official is done in 12 minutes rather than the 31 minutes for normal intercept requests. We can reflect the variation in the 'evaluate request' activity by adjusting time equation (3). This can be seen in the following equation:

(5) Total time for intercepts department = 31 × (volume of normal requests evaluated) + 12 × (volume of warrantless intercept requests evaluated) + 62 × (volume of requests processed) + 82 × (volume of warrantless intercept feedback given)

Capturing this and other variations in activities allows for greater granularity and hence provides more detailed cost information to management.

In the following section we discuss some of the advantages of TDABC over ABC.

5.3.3 Advantages of TDABC

As mentioned earlier, TDABC was developed to help overcome the problems with ABC which resulted in ABC having a low rate of uptake. In the discussion below we group some of these advantages into three areas: cost, ease of use and/or maintenance, and accuracy.

Cost. TDABC is cheaper to implement due to the fact that the TDABC process is simpler. Recall that in Step 2 of the ABC process costs are assigned first from resources to activities. This time consuming and error-prone (Kaplan & Anderson 2007, p.9) step is avoided by TDABC since TDABC uses time to allocate costs directly from resources to cost objectives (Szychta 2010, p.53). In some cases this makes ABC infeasible. For example, Dalci et al. (2010, p.633) report in their case study that it was not feasible to trace activity costs to customers using ABC due to the diverse use of resources by customers. TDABC, however, proved to be a suitable alternative in this case.

TDABC also does not require the regular in-depth employee surveys normally carried out by ABC (Szychta 2010, p.57). The cost and time taken to conduct such surveys "have been a major barrier to the implementation of a traditional ABC system" (Dalci et al. 2010, p.611). In TDABC measurements taken by direct observation, information from workflow systems, or simpler employee surveys can suffice (Kaplan & Anderson 2007a, p.10)(Szychta 2010, p.53). Kaplan and Anderson assert that this is because TDABC requires accuracy but not a high degree of precision.

Ease of use and/or maintenance. TDABC systems are easier to maintain and modify due to the absence of a large activity directory. TDABC is able to capture an activity, as well as any variations in it, with a single time equation. In ABC, each variation is recorded as a separate activity in the activity directory. The implication is that the size of a TDABC model "increases only linearly with real-world complexity, not exponentially, as in conventional ABC" (Kaplan & Anderson 2007b, p.29). In one case an ABC model of 900 'activities' was reduced to a TDABC model of 100 activities (Kaplan & Anderson 2007b, p.29).

Everaert and Bruggeman (2007, p.20) note that when new cost objectives are added, or when changes to resource costs occur in ABC systems this necessitates revising or recalculating the entire cost model. This is also borne out in Szychta (2010, p.51-53). Szychta lists complexity and problems involved in the modification of ABC systems amongst the main causes of dissatisfaction by employees using ABC systems. TDABC is simpler to modify and does not require recalculating or revising the entire model when changes are made (Everaert & Bruggeman 2007, p.20).

Accuracy. In ABC the time estimates reported by employees during interviews usually totals 100%, or full capacity, because employees do not want to report underperformance. ABC cost driver rates are thus based on employees working at full capacity, rather than their practical, or actual, capacity. This results in inaccurate cost information from ABC systems. As mentioned in the previous section, TDABC uses practical capacity – a more accurate measure. The practical capacity of other resources, such as technological resources, can also be estimated by taking into account the expected downtime for maintenance and repairs.

Everaert et al. (2008, p.174) note that ABC uses a single rate for each activity and may therefore provide inaccurate information where multiple drivers are involved – for example, an order processing activity that uses paper based and online orders. Using an average cost for both types of orders distorts the accuracy of the cost information and splitting the activity into two separate activities increases the complexity of the ABC system. TDABC can express this scenario in a single time equation.

Some argue that ABC can be used with time as a driver; however, this still involves the costly second stage of ABC to be implemented. In any event, neither ABC nor TDABC should be considered automatic choices for cost management. The cost of implementation, the accuracy of existing cost management methods and systems in place must also be taken into consideration. We discuss some of these factors later in Chapter 7. For the purpose of digital forensic processes, which usually consist of distinct activities, TDABC is an attractive option since it models the process involved through time equations that incorporate each activity.

In the section that follows we summarise and conclude this chapter.

5.4 Conclusion

In this chapter we discussed the cost system known as Time-Driven Activity Based Costing (TDABC). TDABC was created to solve drawbacks in its predecessor, Activity-Based Costing (ABC). ABC, in turn, was created to address the lack of activity-related information in earlier, traditional costing systems. In order to explain TDABC, we first presented an overview of ABC in which certain key concepts were defined. These concepts included: activities, cost pools, cost drivers, and cost driver rates.

TDABC was then explained. Important concepts in TDABC, such as, capacity cost rate, practical capacity, total activity cost, and time equations were also defined and explained. To illustrate the use of TDABC, a practical example was also presented. Lastly, we discussed the advantages TDABC has over ABC.

The concept of TDABC, as well as the terminology introduced in this chapter will be used later in the thesis when we examine the use of TDABC to manage DFR.

The end of this chapter also marks the end of Part 1 of this thesis that deals with background theory. Part 2, which contains the contributions made in this thesis, follows.