Net privacy policy: its development and implementation as a management challenge

by

PJ Reynders

A mini-dissertation submitted in partial (25%) fulfilment of the requirements for the degree

M COM (BUSINESS MANAGEMENT)

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

RAND AFRIKAANS UNIVERSITY

Supervisor: Prof N Lessing

October 2004

SYNOPSIS

Name	:	REYNDERS, PJ
Degree	:	M Com. (Business Management) (Short Dissertation has 25% weight)
Title	:	Net Privacy Policy: Its Development and Implementation as a Management Challenge
University	:	Rand Afrikaans University
Supervisor	:	Prof N Lessing
Date	:	October 2004

Privacy evolved from a social rights issue of the seventies to a consumer rights issue in the late nineties, brought about by the advent of the Internet, inter-connectivity and e-commerce. Constant technological and global development as well as a lack of the understanding of privacy issues is seen as a constant threat to privacy protection, necessitating legal regulation and technical compliance to security standards. The loss of privacy can result in financial loss or victimisation for the individual. This presents immense management challenges that must be met by organisations to protect privacy. This study investigates the management approach that will enable a company to meet these challenges by developing and implementing a net privacy policy. This management approach employs the four basic management functions as its basis where the planning and organising functions constitute the development phase and the leading and controlling functions makes up the implementation phase.

SINOPSIS

Naam : REYNDERS, PJ

Graad : M Com. (Ondernemingsbestuur)

(Skripsie het 25% gewig)

Titel : Netprivaatheidsbeleid: Ontwikkeling en Implementering as Bestuursuitdaging

Universiteit : Rand Afrikaanse Universiteit

Studieleier : Prof N Lessing

Datum : Oktober 2004

Privaatheid het ontwikkel uit 'n sosiale regskwessie van die sewentiger jare tot 'n verbruikersreg in die laat negentiger jare, as gevolg van Internet en e-handel toepassings. Konstante tegnologiese en globale ontwikkeling tesame met 'n gebrek aan begrip vir privaatheidskwessies, vorm 'n voortdurende bedreiging vir privaatheidsbeskerming. Dit het op sy beurt tot wetlike regulering en tegniese sekuriteitstandaarde aanleiding gegee. Die verlies aan privaatheid kan finansiële verlies en viktimisasie van die individu tot gevolg hê. Die besigheidsomgewing staan dus voor geweldige uitdagings vir die beskerming van privaatheid. Hierdie studie ondersoek die tipe bestuursbenadering wat gevolg moet word om hierdie uitdagings doeltreffend die hoof te bied. Die bestuursbenadering wat die moontlike oplossing kan bied steun op die vier basiese bestuursfunksies, waar beplanning en organisering die ontwikkelingsfase vir netprivaatheidsbeleid vorm en leierskap en beheer die implementeringsfase opmaak.

Net privacy policy: its development and implementation as a management challenge

Contents

Chapter 1: Orientation

1 Orientation

1.1 Introduction

Privacy is a human need that concerns the desire of an individual to keep his personal information that he regards worth protecting, confidential. The privacy of personal information can be threatened or breached in various ways. One of these is the way that business employs technology to realise profits or the way technology is employed by governments for public administration purposes.

Technology used by governments in the seventies helped along the advent of the Information Age (Davies 1997: 145), triggered by the increasing processing and storage power of supercomputers used to track the personal details of their subjects, asking invasive and sensitive questions (Bennet 1997: 103). In the eighties, the foundation for modern computing was laid. Data stored in databanks, became important in itself, once the data was captured into the database, vast quantities of data could be manipulated freely (Vinaja 2002: 284) in an unprecedented way that would have required an army of filing clerks just a few years before (Oberholzer 2001: 12).

Modern privacy issues resemble some of the old but some issues are new:

- Most companies employ databases (as in the seventies) containing vast quantities of personal information of their clients (clients *i.e.* vendors, suppliers, customers) for marketing purposes (Kotler 2000: 108), in an attempt to respond to cyber-consumer demand (Corby 2002: 89).
- E-commerce is on the increase, transactions are done electronically where information needs to be disseminated (Erbschloe & Vacca 2001: 38). Financial and other personal details must be submitted to validate and complete the transaction and can create privacy concerns in the process.
- Boundaries virtually vanished with inter-connectivity and web-browser technologies (Samarajiva 1997: 278) connecting not only PC's but, PDA's,

televisions, fridges, cell phones, cameras and other electronic devices that share information on an unprecedented scale (Vinaja 2002: 282).

- Consumers are bombarded with advertisements, promotions and offerings through all possible delivery channels, including SMS-advertising, e-mail, spam (Gupta & Sharma 2002: 5) and Web banner-advertisements (Whittaker & Sidner 1997: 280) to name but a few. Little thought is given to whether people actually want to be reached in this way, as much of this constitutes a serious invasion of privacy.

The aforementioned technological developments changed consumer patterns and subsequently transformed privacy from a purely political social rights issue of the seventies (Steel 1979: 4) to a consumer-rights issue in the late nineties (Davies 1997: 143). As a consumer issue today, privacy has lost little of its former political and social sensitivity but poses whole new management challenges not encountered before. Organisations need to find ways to protect private information. It makes *good business sense*:

- DoubleClick lost 20% of its market value in only three months after privacy advocates publicised the company's questionable practice of using cookie technology to track users' web surfing patterns and connecting anonymous cookie information with real-life identities (Gupta & Sharma 2002: 2). Succumbing to market, public and political pressure, DoubleClick revamped its policies (Erbschloe & Vacca 2001: 16-17).
- Easyinfo listed Telkom's unlisted telephone numbers in their Internet Information Directory. Telkom claimed that it did not provide Easyinfo with the data directory and was concerned about the way their clients' information was obtained. After some public outcry, Easyinfo agreed to remove these listings from their web search facility. Easyinfo refused to apologise for presenting accurate information, nor did they disclose the source from where they obtained the data. They only apologised if they offended any members of the public (Lotriet 2002: 1).
- In 2003, an unidentified South African bank disposed of a few thousand personal computers containing confidential information and software, resulting in financial

liability and loss. Much of the information was gathered through transactions over the Internet (Sake Beeld 2003: 13).

Good business sense should not be the only motivation for protecting clients' privacy but should also include *moral and ethical considerations*:

- Medical history for instance should be kept private and secure as individuals can be seriously compromised or victimised if some of this information is leaked (Oberholzer 2001: 62).
- Clients' bank account details, which if leaked can result in material loss, resulting in liability to the negligent company (Opperman 2003a: 1).
- In other instances, the loss of privacy can lead to dysfunctional and unnatural behaviour as demonstrated by the Apple Virtual Café Experiment where employees were subjected to extreme invasion of privacy through acute surveillance and all other means of privacy invasion (Belotti 1997: 75-76).

1.2 Problem definition

The introduction illustrated the need for companies to protect the sensitive and private information of their clients. The management challenge lies in the way that companies will choose to protect this information. To achieve this, companies will need to handle privacy issues through a structured management approach. Studies abound on technical privacy issues (Dreyer 1999: 9, Oberholzer 2001: 76), legal privacy aspects and other issues (*c.f.* Fazlollahi 2002; Erbschloe & Vacca 2001) concerning privacy. None of these investigated managerial issues concerning net privacy policy management. Erbschloe & Vacca (2001) came closest to establish some sort of a managerial process for protecting privacy. Their approach however explicitly stated that they merely attempt to establish a guide towards building ironclad net privacy policies.

The research problem that this study will therefore investigate is the establishment of a structured management approach to assist companies in meeting the management challenges posed by the need for protecting the

private information of their clients through the development and implementation of a net privacy policy. To fully address the problem as stated, the following *related problems* must be addressed:

1.2.1 Problem 1 – Privacy issue definition

In order to meet and understand the challenges posed by the need for protecting privacy, a good understanding of privacy issues is required. *Privacy definitions, legal*, *ethical* and *technological* issues all impact directly on privacy and need to be accounted for.

1.2.2 Problem 2 – Privacy management challenges

There are specific challenges facing managers, generated by the relevant privacy issues, never encountered before. It is therefore important for companies to ascertain the extent and nature of these *challenges*. These challenges present themselves in the form of *understanding the economic impact of privacy, security and risk management, managing the way people interact with technology* and *managing customer satisfaction* in a rapidly changing world.

1.2.3 Problem 3 – Management approach

In order to manage privacy issues effectively, a *management approach* must be selected. The *management approach* to be chosen will have to be one that will enable a manager to meet the *management challenges* identified. It will therefore have to be a *multi-disciplinary approach*, contain *project management elements* due to its multi-disciplinary nature and have the *four management functions* as its basis.

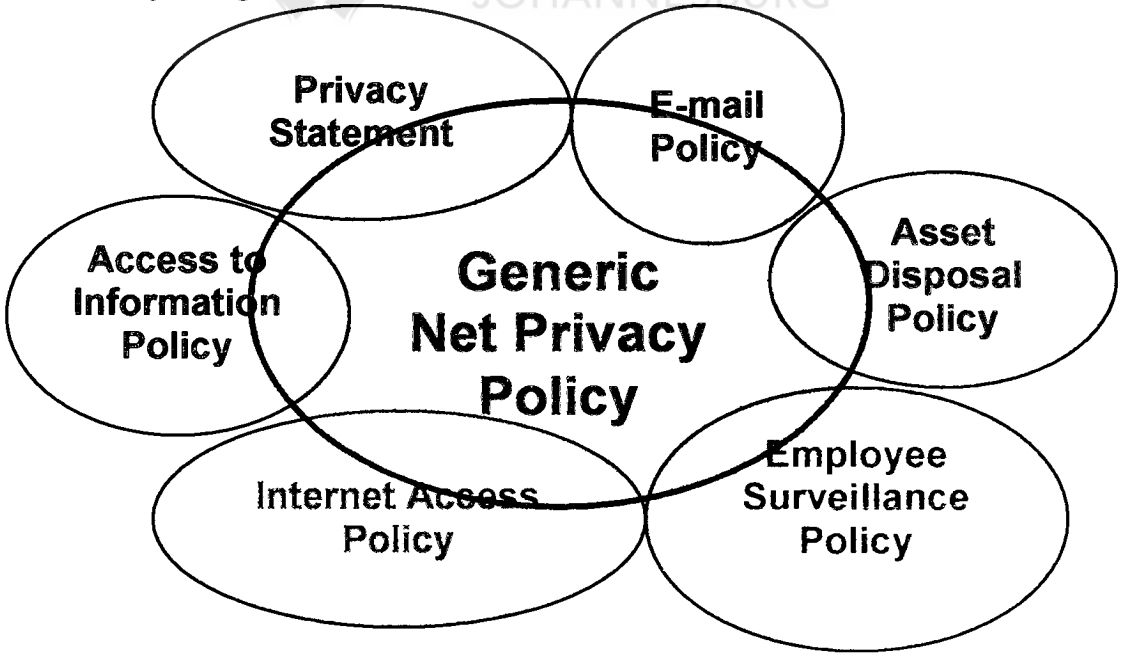
1.2.4 Problem 4 – Management approach application

Choosing a management approach does not solve problems unless it is quantified into workable applications. The problem here lies with applying the *management approach* in a practical sense that can assist in the *development* and *implementation* of a net privacy policy. This occurs in two distinct phases, a *development phase* consisting of the *planning* and *organising* functions and an *implementation phase* consisting of the *leading* and *controlling* functions.

The scope of the study can be demarcated as follows:

- The focus is confined to the management challenges posed by the development and implementation process of a net privacy policy. Because management problems are in most instances uniform, this study will address the generic management issues.
- No attempt to exhaust the legal and technical issues will be made but will treat these where they bear relevance to the problem at hand.
- Defining privacy in an exhaustive way is not the aim of the study but it attempts to define privacy in a business context to illustrate its relevance to the management challenges.
- Privacy is a complicated issue and impacts on several other issues addressed in policies within any organisation. The focus will remain with the privacy policy only and will briefly refer to others where relevant. It can be graphically illustrated as follows:

Figure 1 – Policy integration



This study is therefore of a limited scope but this does not impact on its specific scientific outcomes. The current study focuses on a very small field within the broader scope of privacy management and attempt to address an issue not

sufficiently covered in existing literature. Its finely demarcated scope therefore correlates well with the specialised and small field of net privacy policy.

1.3 Research objectives

The main objective of this study is to *determine and define privacy issues* that constitute *the management challenges* facing privacy protection within an organisation and how the design of *a structured management approach* can provide a *practical solution for the development and implementation of a net privacy policy.*

1.3.1 Objective 1 – Determine related privacy issues

In order to ascertain the management challenges, one first needs to determine the *related privacy issues* that create a management challenge. In **chapter 2** a literature study was undertaken to determine *privacy definitions, the legal, ethical, technological* and *security issues* that all impact directly on privacy.

1.3.2 Objective 2 – Determine the privacy management challenges

The complicated and diverse issues referred to under 1.3.1 are of a multi-disciplinary nature, as is attested by the multi-disciplinary nature of the literature consulted. A huge *management challenge* is posed to the organisation in the way that it will manage the diverse challenges presented by *understanding the economic impact of privacy, security and risk management, managing the way people interact with technology* and *managing customer satisfaction.* This creates the need for well-informed decisions and a knowledgeable holistic approach. In **chapter 3**, the management challenges as determined by the privacy issues defined in **chapter 2**, will be identified.

1.3.3 Objective 3 – Determine a management approach

Once the management challenges are identified, it will be possible to determine what type of *management approach* should be used to address these challenges. In **chapter 4**, a suitable management approach will be investigated and identified that is flexible enough to accommodate *multi-disciplinary elements*, contain *project*

management elements due to its multi-disciplinary nature and have the *four management functions* as its basis.

1.3.4 Objective 4 – Determine a structured approach for the development and implementation of a net privacy policy

Once the *management approach* is identified, it will be possible to determine a practical approach for *implementing* and *developing* a *net privacy policy*. The *development* and *implementation* are two distinct phases within the policy process. **Chapter 5** will investigate the *development phase* where the *planning* and *organising functions* are constructed by *vulnerability, data audits, risk analysis* and *legal framework* and *privacy policy element* identification, respectively. **Chapter 6** will determine the *implementation phase* where the *leading* and *controlling phases* are made up of *communication strategy*, *training* and *process effect controlling*.

1.4 Methodology

A *qualitative approach* was followed in order to achieve the research objectives. Since there is a lack of understanding the impact of privacy (Agre 1997: 22) it would not serve any purpose to conduct interviews through sampling. Ample literature concerning the various aspects of privacy exists but none fused the various elements into a structured management approach. A *literature study* was therefore chosen:

- To provide a theoretical basis for privacy issues. Privacy issues cannot be understood without a theoretical basis.
- To account for the related issues relevant to this study, concerning privacy.
- To establish a structured approach that can assist in meeting the managerial challenges when constructing a net privacy policy.

Literature was selected based on the following *criteria*:

- Dated literature was chosen only if it could help to form a theoretical base and to illustrate the development of privacy issues to accentuate the ever changing and diverse nature of privacy problems.

- Recent literature was chosen to illustrate the implications of real-life examples to privacy issues and which could establish a structured approach for meeting the management challenges surrounding privacy policy development and implementation.

1.5 Closure

The need for privacy exists everywhere but the way in which technology touches humans' everyday lives makes the issue even more acute. Submitting private and confidential information over the Internet, poses new challenges in the way this information is disseminated by the company that holds the information. A need therefore exists to handle these privacy concerns in a satisfactory manner. Herein lies the contribution of this study in that it attempts to determine a practical and structured management approach for developing and implementing a net privacy policy that can assist in limiting liability and risk, and provide workable solutions for protecting privacy.

Chapter 2: Determining privacy issues

Synopsis

This chapter investigates the *related privacy issues* surrounding privacy and the most important implications for organisations that ultimately pose a challenge to management. A literature study was undertaken to determine these issues and were identified as *privacy definition, net privacy, technological issues* as well as *legal and ethical frameworks* that all impact directly on privacy.

Each of these aspects was investigated to determine their extent and implications. A *privacy definition* is important to demarcate the boundaries of responsibility and activity for a company. Within that definition, *net privacy* can be defined as a subset of privacy and properly demarcated. *Technological* and *security issues* all relate to the challenge of providing physical hedges for protecting privacy. *Legal* and *ethical issues* are treated within the given legal frameworks within which a company operates as it can involve more than one country especially in the case of multi-national enterprises.

Once the scope of these issues can be determined, the full extent of the management challenges can be ascertained.

2 Determining privacy issues

2.1 Introduction

The introductory chapter determined the most pressing issue concerning privacy, namely that *technology* presents a clear and present danger to privacy. Each organisation also operates within a *legal framework* and sometimes in more than one, depending on whether the organisation only has localised operations or whether it is a multi-national organisation. Privacy differs in meaning from country to country in customary terms and is legally specified depending on the locality. It is therefore important to understand what is meant by a definition of *privacy* that can be extrapolated to *net privacy policy*.

In a business environment the *legal* and *technological issues* impacting on privacy, are the most important. Issues relating to the legal framework, within which privacy is protected, also include *ethical aspects*. These are more difficult to define and people within an organisation may at times be widely divided on what constitutes *ethical behaviour* concerning privacy. There is a real danger of simplifying privacy issues, namely that *legal* and *technical issues* are the only relevant ones. Most organisations indeed think that privacy policy revolves only around securing a *legal* and *technical* hedge to protect the companies' exposure to liability (Holvast 1993: 267).

Compounding the problem is the fact that legal frameworks address only the legal and technical legal issues, ignoring the broader social political contexts (Bennet 1997: 101) as well as the managerial process. Even in recent literature, the *management process* is given a backseat (see chapter 1). The implications of these issues present the management challenges. Once an organisation has determined how the abovementioned issues impact on privacy, the management challenges can be defined and planned for.

2.2 Privacy definition

In order to address privacy issues, an organisation at least must have some sort of a definition for privacy. Attempting to exhaustively define privacy is a study in itself. A normative definition of privacy will be sufficient and it stipulates that at least some of a person's activities, information and nature should not be available for public consumption, where a person has the right to be left alone (Gupta & Sharma 2002: 2), where some of the norms are stipulated legally and can differ widely from country to country in legal and customary terms (Belotti 1997: 66 - 67). With this in mind, *privacy* here denotes private personal information of individuals, which can also include legal personas such as companies that constitute legal entities. *Personal information* is information that reveals a distinctive trait about yourself and helps others identify you (Proquest 2004a: 3): It relates to any sensitive personal, medical or financial data that may place the individual (read person or legal person) at risk, liability or embarrassment.

An issue closely related to privacy concerns the issue of *information ownership* (Erbschloe & Vacca 2001: 2; Ware 1979: 15). Information can belong to companies or individuals but disseminating this information does not necessarily imply that ownership is abdicated (Miller 1971: 48, 212). Individuals disclose personal information to banks to obtain loans or individuals might disclose personal information to gain access to websites. This does not imply that they give consent for their private details to be distributed or sold to the highest bidder. Although privacy today is a consumer rights issue, it should be kept in mind that privacy itself is not a commodity that can be traded. Consumers are persons with a right to and a need for privacy and they pay for their goods and services with money, not with their privacy – privacy is not a currency.

Branching out from the issue of *information ownership* is that of the right to have freedom to and *access to information.* This raises the question of where does the right of privacy start before it infringes on the rights of others, that exercise their right to have access to information. This can create an interesting conflict of interests. A

legal framework regulates both *privacy* and *access to information*. An organisation should determine the legal boundaries of each and the peripheral points of commonality, relevant to its own situation.

2.3 Net privacy

We have determined that the way in which technology is used, private information of persons or companies can potentially be threatened through business transactions. Some of the most common ways of disseminating information are through e-commerce or web surfing. In order to effect an e-commerce transaction or visit a website, private information must be disseminated. The question revolves around the way that this private information is transmitted, stored or disclosed to third parties or in other ways. Web sites collecting information by whatever means for whatever purpose, post a *privacy statement* on their website. The user can view this statement that informs him about the way his information is used. This should not be confused with the *net privacy policy*, as is most often the case.

A *net privacy policy* is far more encompassing than a *privacy statement* and is an internal policy document that the company institutes to guide the way that private information is disseminated through the business processes in the company. It bears relevance to every other policy in the company that entails the dissemination of private and confidential information (see Figure 1). The implications of each of these are complicated and should be carefully considered. The *privacy statement* should be the part of the *net privacy policy* that relates directly to the individual person or legal person's information that is collected from the Internet.

It is important that the privacy of such individuals is protected and guaranteed by a policy that is communicated right through the organisation to all levels. Communication alone is not enough. The net privacy policy needs to be respected and upheld by its employees to their own benefit and that of the company. A net privacy policy subsequently not only protects the individual but it also indemnifies

employees, protects the company and extends credibility to the company's business ethic.

2.4 Technological issues

Business as part of the universal human endeavour employs data and personal information stored through indispensable computer technology (Hutt 1995: 1.3) to realise profits. Transactional and personal information is stored for this purpose in vast data-warehouses that can be freely and easily distributed (Anderson & Post 2000: 299, 343). Technology in general is therefore perceived to be of an increasingly intrusive nature, constantly infringing on personal privacy (Agranoff 2002a: 3). Having such information and technology as such is not necessarily undesirable but the way it is used or disseminated represents the core of the problem and creates the concern of how this data will be used in future.

This technological interaction between business and the individual, whose privacy is involved, creates the privacy concern. Focusing on the darker side of technology though tends to obliterate the positive role that technology can play in protecting privacy. The use of soft- and hardware to protect privacy with a technological hedge is big business. Compliance with security and industry standards such as ISO9977, COBIT and ITIL is necessary and can contribute towards creating a safe environment where privacy is protected.

Relying on technology alone is problematic. Miller's approach, although dated, still bears relevance. He rejected the belief in technology as the ultimate means of protecting privacy. At the time telegraphs and wireless communications were deemed to be the ultimate way of safe and private communication, which of course was not true. He prophetically foresaw that technology would never be able to provide totally secure and private means of communication (Miller 1971: 27). Even today, companies have to find increasingly ingenious ways of protecting their own information as well as that of their clients. This is despite all the technological advances on security management.

2.5 Legal and ethical issues

Bankrupt American airline companies sold databases with confidential and private data because they deemed these to be disposable assets, despite the very existence of laws specifically prohibiting these types of transactions. This sparked huge public and political outcry and was stopped by the intervention of the court (Carroll 2002: 49-50). Managers made these decisions but is clear that they either had no idea about the existing laws or that they maliciously intended to do so, resulting in unethical behaviour. This once again underlines the importance of a net privacy policy that not only informs clients but also guides the managers and other employees who are the gatekeepers of privacy.

In creating a net privacy policy, companies will need to ascertain the legal framework of the home country or the foreign countries where they operate if they are multi-national enterprises. It is a very likely scenario that privacy laws of two different countries wherein a company operates can have diametrically opposing privacy laws. This constitutes an immense legal and managerial challenge, as is the case in the US.

From a moral and ethical point of view, one needs to question the ethics of companies like Double-Click and Easyinfo who continued unrelentingly with activities that were unacceptable to the public and their customers. It defies comprehension how they could justify these wholly unacceptable activities. The making of profit can never supersede the moral and ethical conscience of society. Business is part of society and therefore also part of its moral and ethical framework. While the chasing of profit may yield short-term gains, it can be very costly in the long run. Due to a rise in consumerism, one sees that informed consumers does not buy products or services which has been produced in an unacceptable way, was illegally required or is harmful to the environment. In the long run these companies will suffer a serious loss of business and good reputation.

Agranoff (2002a: 11) refers to the ethical aspects as those not covered by (American) law and uses the example of the lack of a legal framework guiding the existing custom of employee e-mail surveillance. Here the principles of fair play, fair chance and proper communication hold sway in the absence of a legal framework. This is especially true in America where a patchwork of federal laws guides privacy protection and no single set of regulations exists (Oberholzer 2001: 31). This very same principle can be used in a generic sense in the absence of a sufficient legal framework anywhere in the world and can guide the legal aspects of a net privacy policy.

In South Africa there are existing legal provisions that must be accounted for in the net privacy policy since it has direct bearing on privacy issues:
1996 – South African Constitution (108/1996).
1998 – Open Democracy Bill (67/1998).
2000 – Promotion of Access to Information Act (2/2000).
2002 – Electronic Communications and Transactions (ECT) Act (25/2002).

The OECD (Organisation for Economic Cooperation and Development) is deemed to be the leading international organisation that is addressing privacy issues and provided the basis for much of the EU-legislation on privacy (Erbschloe & Vacca 2001: 30). The EU's Directive on Data Protection requires that transfer of personal data only occur tot non-EU countries that have acceptable levels of privacy protection. With the EU as South Africa's biggest trading partner, this has an adverse impact on how privacy legislation is enforced and adhered to. This has resulted in the creation of Safe Harbour Principles where organisations can voluntarily submit to these principles and note their compliance to these in their *privacy statements* and *net privacy policies.*

The ECT Act made electronic signatures legal as admissible evidence in a court of law. This implies *e.g.*, that in the event of a person visiting a website, accepting the legal terms and conditions and the organisation collecting his private information should disseminate his information in contradiction with the electronic agreement, the organisation would be in breach of contract and can be held legally liable.

2.6 Closure

Before attempting to address *privacy issues*, an organisation needs to have some sort of a definition of *privacy* that can be legally stipulated with *net privacy* as a subset of this definition. This can create a complicated situation where it becomes difficult for organisations, their managers and employees to make judgement calls upholding the privacy of individuals whose information they possess. The most complicated privacy issues are the roles of *technology* and the *legal framework* or *frameworks* within which the company operates. In the absence of a legal framework, *ethical* considerations hold sway to guide the decisions of organisational managers. The subsequent management challenges posed by these issues are immensely complicated and will be discussed in the next chapter.

Chapter 3: Determining the management challenges

Synopsis

The determination of relevant *privacy issues*, lays the platform for the identification of specific *management challenges*. This chapter investigates the details of each *management challenge* that is generated by the relevant *privacy issues* as determined in the previous chapter.

The complicated nature of privacy issues asks for a multi-disciplinary approach due to the fact that privacy issues cut across so many disciplines. The specific management challenges that arise from *privacy issues* firstly concerns *security* and *risk management* that can provide physical hedges for privacy protection and how to ascertain risks to privacy. *Technology* can protect privacy but also threaten it in the way with which *people* interact with it. The real challenge arises from the synergy to be achieved by combining them. Certainly the greatest challenge is the way that *customer satisfaction* is achieved. Only through a continued relationship embedded in trust, can e-commerce grow if the individual is confident that his privacy enjoys protection. This relationship of trust can create a competitive advantage for the organisation concerned.

3 Determining the management challenges

3.1 Introduction

Technological and *legal issues* are the most important issues concerning privacy out of which management challenges arise. A general lack of understanding exists concerning the *economic impact* of privacy (Agre 1997: 22) and it is therefore difficult to manage that which one cannot quantify. The manufacturing of technology is an exact science but its application to business, through human intervention, muddles the lines of clarity and subsequently its impact on privacy. An organisation must attempt to fully understand all the relevant issues concerning privacy.

Harnessing the potential of technology and a legal framework through human resources, represent the core of the management challenge. People within the organisation need to apply technology correctly and act in terms of the prescribed legal framework:

'No matter how well crafted a privacy code might be, privacy will only be protected if the necessary information practices are actually followed'. (Agre 1997: 25).
The challenge for the manager lies in the way that he plans, organises, leads, control communicates, and trains throughout the management effort. When done correctly it will be possible to integrate the human effort with technology and the legal framework.

The management of privacy is a *multi-disciplinary effort.* This already became evident in the preceding chapter where it was emphasised that there are a myriad of issues that impact on privacy. Only a well-informed management team guided by a capable, well-educated manager will be able to develop and implement a well-crafted privacy policy. Project management is designed to provide an umbrella for managing wide ranging disciplines within one project. This type of approach should take care of the needs that a multi-disciplinary project requires. This is also emphasised by

literature on privacy where almost each and every publication was contributed to by a host of authors from different backgrounds and disciplines.

3.2 Privacy, security and risk management

There is a very important link between *privacy* and *security*, though the two issues are often confused (Oberholzer 2001: 13). Where privacy concerns the concept of what is held to be private and sacred to the owner, *security* represents the *physical protection of privacy*. Security therefore represents physical, technological, legal and managerial barriers designed to protect the private information of the stakeholders. Without proper security, there can be no privacy. Security, though, is often breached (Gupta & Sharma 2002: 3). If the people in an organisation, entrusted with the protection of private or sensitive information, through security measures, do not respect the privacy they are suppose to protect these security measures are redundant. They possess the passwords, access cards, biometric access or technical know-how to access this information. It is therefore of primary importance to recognise that not only the technical security are viewed as an integral part of the privacy policy making process. Employees also need to respect the information and the parties this information belongs to that they are supposed to protect.

The management of *privacy* and *security* is directly related to *risk*. The role of security concerns the protection of data security systems. Data as an asset as well as the technical and other security systems are the manageable assets of the company and must be safeguarded by management (Hutt 1995: 1.5). Management needs to determine the magnitude and probability of risk in managing privacy. This presents a management challenge in itself, since it is very difficult to determine the privacy risk elements, their probability and economic magnitude.

Increased Internet traffic and transactions inevitably lead to increased risk (Carroll 2002: 50) and a need exists to manage or ascertain this risk. A paradigm or management structure is required to handle the protection of privacy. Risk management with its close relationship to privacy, constitutes a management

challenge. If the risk is determined and properly identified and subsequently well managed, it can reduce the risk to the organisation. E.*g.*, if the net privacy policy states that the private information of individuals will not be disclosed under any circumstances, this should also reflect on the disposal of assets policy (refer to the example of the anonymous South African bank under 1.1).

3.3 Managing technology and people

The importance of a net privacy policy should force organisations to follow a management process that includes amongst others technological and legal issues in order to account for the human factor, which is the greatest risk to privacy (Corby 2002: 85; Holvast 1993: 273). The privacy of employees is very often neglected. Employees are the only sustainable resource of any company and should be treated with the same respect and dignity as customers. Network software exists that can monitor employees' e-mail, their web navigation habits as well as their performance levels. Network monitoring software existed for a very long time. Since the times when IBM and Novell had a monopoly on network systems, network management systems (NMS) were already available, but its use very soon extended to monitor employee activities at the time (Stamper 1994: 462).

Sometimes these activities are posted on bulletin boards to promote better performance. The same kind of issues arises with closed-circuit-TV and other monitoring technologies. Although this is legal in some countries, it occurs mostly without the knowledge of the employees themselves. Employees can incriminate themselves unknowingly, whilst they might not have done so if they knew that they were being monitored. Some question the managerial value of such actions (Anderson & Post 2000: 597). Management must instate policies to regulate the e-mail and other activities of employees (Capuder 2002: 23). This is also very closely connected with the privacy of individuals although they are employees in this case. The employer itself should set the example on privacy protection so that the employees will follow and implement these principles themselves in their everyday tasks

It does not require a genius, as is widely accepted, to commit input fraud and falsify records and claims (Bologna 1995: 6-9). It is very often an insider who provides just enough assistance for an external perpetrator to penetrate a company's network or they commit security and privacy breaches themselves. Employees must, therefore, come to understand and respect the privacy of personal information that will in the end benefit them as well.

Apart from impressing the need on employees to safeguard private information kept by their employer, they also need to understand that they themselves can be a risk to privacy. Humans do make mistakes and information can be divulged or damaged by sheer stupidity and not only malicious intent (Miller 1971: 32-33). Technology can limit human errors but never eliminate them. The protection of privacy reaches further than just the afore mentioned end-users committing mistakes. Many times, systems are designed in a privacy unfriendly manner. Privacy issues always lose out to system functionality leaving those whose privacy has been compromised, asking the question: 'How did they get my name? (Agre 1997: 56).

This emphasises the need to manage and train all employees within an organisation, ranging from the lowly data-capturers to the highly skilled programmers, who are not always necessarily sensitised to privacy issues. It follows logically that neither of these groups of employees, or any other, can be approached or trained in the same manner. The immensity of the management challenge lies in the fact that all the implications must be assessed, understood and transferred meaningfully to the employees on their different levels.

3.4 Managing customer satisfaction

Protecting the privacy of customers is of paramount importance. This becomes all the more important where business-to-business transactions are done through the Web. Providing security is the responsibility of the service provider. The risks are well known and should be eliminated for the benefit of the consumer. Most

companies engaging in the dissemination of information through the Internet post privacy statements on a visible part of their web page. Contained in the privacy statement it should be stated exactly what the company intends to do with the data of their customers be it individuals or other companies (Anderson & Post 2000: 597). Every other consideration aside, having such a policy makes good business sense. Assuring consumers and proving that the privacy policy is actually enforced is the best way of buying social co-lateral from your customers. Businesses should therefore be encouraged to use privacy enhancing technologies to the best benefit for their customers (Agre 1997: 24).

A potential customer will never engage in e-business if he does not trust the source. Thus the reason why the global growth in e-commerce is lower than first anticipated (Papazafeiropoulou & Pouloudi 2002: 33). Customers must be assured that their privacy will not be breached nor will their financial details such as credit card details be disclosed to other parties. This will ensure that the customer will be back for more business and will experience satisfaction. This is extremely important from a managerial point of view, because it can potentially improve profits and produce return business that costs much less than recruiting new business. Trust is linked to loyalty and is built over time through repeated experience, if a customer trusts a website he will return (Tomluk & Pinsonneault 2002: 95). In a recent survey done on participating companies engaged in b-2-b-transactions (business-to-business), privacy and security were ranked as the most important factors of the process. Trustworthiness was also ranked as important and it is therefore imperative that companies adhere to its confidentiality and privacy policies (Griffin *et al.* 2002: 274).

3.5 Closure

The difficulty of the *management challenge* can be summarised as that the protection of privacy requires a multi-disciplinary management approach that can provide *security*, accurately assess *risk*, *manage and train people* in the way they use *technology* that will ensure a credible environment for e-commerce (read dissemination of information over the Internet) thus securing *customer satisfaction.*

Privacy today is a consumer rights issue, a direct result of e-commerce. The management challenges revolve around the way that privacy is protected, especially in an environment where information is disseminated over the Internet through b-2-b or b-2-c (business-to-customer) transactions. The way that organisations deal with privacy will therefore ultimately determine the future of e-commerce. If consumers can invest trust in the Net Privacy Policies of organisations, e-commerce will grow. Managers will have to realise that trust cannot be bought but must be earned through a continuous relationship.

Relying on a legal framework and technology alone will afford privacy protection only to a limited extent. It was shown earlier that privacy can still be compromised in the presence of a legal framework and that technology as such can also threaten privacy – either through its internal design or the way it is employed by humans. Active human effort is required and it is exactly this effort that creates the *management challenge*. Management is an active human effort and the type of management approach that can sufficiently meet the aforementioned challenges will be discussed in the next chapter.

Chapter 4: Determining a management approach

Synopsis

In this chapter, the *management issues* surrounding privacy will be used to determine the nature of the *management approach* that will be needed to address them. It will take a very brief look at the required elements that must be inherent to this process and focus especially on the *multi-disciplinary* nature of the process.

The chosen *management process* is based on the *four basic management functions* of *planning*, *organising*, *leading* and *controlling*. These four functions also represent *phases* in the management approach. *Planning* and *organising* comprise the *development phase* of a *net privacy policy* whilst *leading* and *controlling* makes up the *implementation phase*. The *multi-disciplinary* nature of the process requires a *project management approach* that was invented in the first place to manage projects consisting of diverse and *multi-disciplinary* dimensions. The project management approach will become the driver of the *four basic management functions* that will provide the framework for the manager in which he can manage the process of *developing* and *implementing* a *net privacy policy*.

4 Determining a management approach

4.1 Introduction

An organisation has to deal with the management challenges generated by privacy concerns. These issues present management challenges that must be dealt with. In order to deal with these issues and challenges as identified in the previous chapters a suitable management approach is needed that possess the following characteristics:

- Flexible to be applicable to almost all situations where privacy issues are managed. It must be able to integrate the various fields and disciplines.
- It must be a generic process to ensure the required flexibility.
- It must be of a multi-disciplinary nature to incorporate all the legal, human and customer related issues as identified in the previous chapter.
- It should take cognisance of project management elements as some wide-ranging (multi) disciplines needs to be incorporated into the process.
- It is an iterative process due to the ever-changing global, technological and legal environments.

For the process to be successful it must posses the following inherent requirements, regardless of its characteristics:

- ***Firstly***, the involvement of employees is essential and it stands to reason that it be accounted for in the process. Employees will ultimately be responsible for enforcing the net privacy policy. They must *respect* the policy and its contents. It is just not good enough for management to *understand* all the issues. The employees in operational units are crucial links in the chain. It is at operational level where the privacy breach can occur, as the examples of chapter 1 illustrate and not only on managerial level.
- ***Secondly***, the implementation and development of a net privacy policy is a managerial function governed by the four basic management functions (Bateman & Snell 1999: 6-8; Gibson *et al.* 2000: 16-18) of planning,

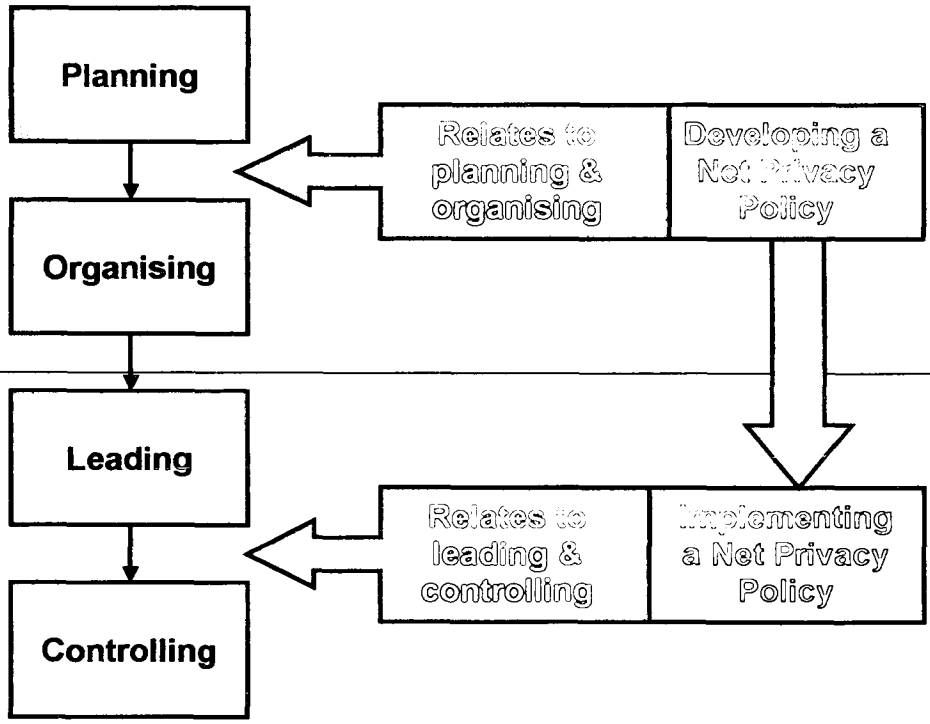
organising, leading and controlling. These are the generic functions found in all management processes.

- ***Thirdly***, the successful development and implementation of such a policy will definitely provide the responsible company with a competitive advantage. The company can potentially be free from legal action, bad publicity and costly litigation (Santos 2000: 1). Without proper privacy protection consumer confidence in e-commerce will erode and so will the growth and opportunities for e-commerce diminish (Carroll 2002: 51). Furthermore, doing business ethically is important and makes a lot of sense (Bateman & Snell 1999: 152). In the case of DoubleClick (see chapter 1), unethical behaviour led to a real decline in profits and market value of its share price.

4.2 Determining a management process

The four management functions as determined under 4.1 will subsequently be used as a conceptual framework for the process of developing and implementing a net privacy policy. Conceptually they integrate as follows:

Figure 2 – Management process



Any balanced management process includes these four basic functions albeit in different terms, the process remains the same (Hitt *et al.* 2001: 6, 37). These four functions also represent the management sub-phases of the development and implementation phases. Each management phase in turn can consist of the four different functions or at least some phases that closely resemble these. Planning and organising can include its own phases or sub-functions of planning and organising. A good example is macro-environmental scanning where the external environment is analysed for strategic planning (Bateman & Snell 1999: 53). The macro-environmental scanning belongs to the planning and organising phase of strategic management but the process itself consists of these four functions. The same functions apply to managerial decision making and strategic management planning (Bateman & Snell 1999: 83, 125, 131) or strategy implementation as well as adaptation.

The *planning* phase is certainly the most important phase. If done correctly, it will lay the path for the rest of process. It should, therefore, receive ample attention so that most of the *organising* will already have been done during the planning phase. The *leading* and *controlling* phases are most often neglected and especially the *controlling* phase. In most instances, too little is spent on the controlling phase (Kotler 2000: 696). Managerial control is seen as the most important step towards achieving a company's goals or a management strategy (Bateman & Snell 1999: 542). The planning and controlling functions are therefore the most important in the process.

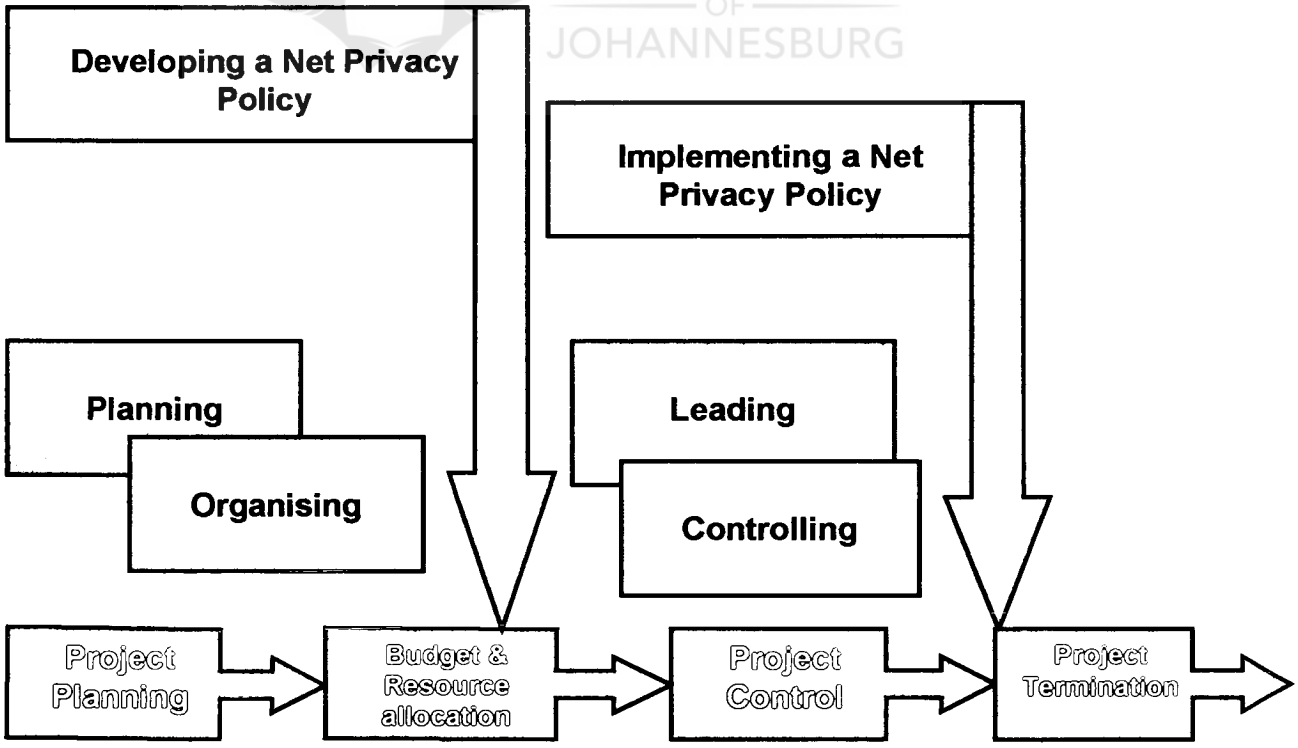
4.3 Project management in the management process

The project management approach can be seen as the driver of the management process. It is the vehicle that is supposed to deliver the desired outcomes of the management process that must ultimately protect private and confidential information. The reason why project management should be used to drive the process is due to the *multi-disciplinary* nature of the management problem, referred to in 4.1. In the previous chapter it became evident that a vast range of management

issues confronts the manager charged with the task of ensuring that private and confidential information is protected. Project management emerged as a way of managing complex and diverse management problems of a *multi-disciplinary* nature where the project manager must be a facilitator and a generalist. Meredith & Mantel (2000: 89) underscores the necessity of the project manager to be able implement the four basic managerial functions of *planning*, *organising*, *leading* and *controlling* throughout the project management process.

The specific needs of an organisation as well as its structure will determine what type of project management model will be used. A functional organisation will pose a wholly different challenge as opposed to that of a matrix or a project organisation. This once again emphasises the need for a capable, well-educated manager who is able to coordinate a *multi-disciplinary* effort. The role of the project management effort that acts as a vehicle for the management process, can be illustrated as follows:

Figure 3 – Project management process



4.4 Closure

This chapter demonstrated that the unique management challenges posed by privacy issues, requires a *management approach* to be resolved and handled within the organisation. A *management process* consisting of the four *basic management functions* of *planning*, *leading*, *organising* and *controlling* can provide the solution. The very nature of privacy issues, require a *multi-disciplinary* approach as shown in this and the previous chapters.

The *multi-disciplinary* approach's needs are best served by a *project management* approach that can drive the abovementioned process and act as a vehicle to deliver the desired results. Project management abides to the same principles of the *four basic management functions* but it can also serve as an umbrella for the integration of complicated and widely different disciplines. The next chapter will investigate the *implementation phase* and more specifically the *planning* and *organising functions.*

Chapter 5: Privacy policy development phase

Synopsis

The chosen *management process* constitutes the *four basic management functions* that underlie all management processes. The *project management approach* acts as the driver for these management functions in turn. The details of each one of these management functions will be investigated and the way in which they integrate into the whole process. The first two functions, namely *planning* and *organising* which makes up the *development phase* will be defined

In the *planning phase* the *vulnerability audit, risk analysis* and *data audit* will receive attention since they indicate the relative problematic areas in the organisation. In the *organising phase*, it is not only important to select others to assist in the process or to assemble the resources, but it is also imperative that the *legal framework* and *privacy policy elements* be identified.

5 Privacy policy development phase

5.1 Introduction

For the process of net privacy policy development and implementation to be successful, the following pre-requisites are essential:

- It needs to have the support of top management. Without top management being pro-active about privacy protection, the process will not be successful (Santos 2000: 2). Management's security policies will provide the pointers for the level of importance it holds within the company and the financial position it holds in terms of budgetary priorities (Abrams & Podell 1998: 111).
- Employees on all levels must be part of the process and respect the need and importance thereof.
- The uniqueness of the organisation must be taken into account when developing the policy since a one-size-fits-all approach is unlikely to succeed (Santos 2000: 3).

Once the pre-requisites are established, the manager responsible for the process can commence the *planning* and *organisation*. Each of these functions, representing phases consists of pre-defined elements. The planning phase provides a platform from which to launch the organisational phase. The planning phase will provide the definite and detailed elements required for organising. Proper attention to these, will pave the way for the rest of the process.

5.2 Planning

The planning function concerns identifying and specifying the goals to be achieved and forms the first part of the development phase. To plan for net privacy policy development and implementation, the manager in charge will have to determine the extent of related issues that will have to be reflected in the policy. An essential part of the planning process comprise the undertaking of audits to determine the extent of

vulnerability to which the organisation is exposed to, the different types of data that exist within the organisation and the consequential risk it is exposed to. This is determined by conducting a *vulnerability audit* (includes technology assessment), a *data audit* and a *risk analysis* that can yield the following benefits:

- They will identify business processes that might possess inherent weaknesses that can put sensitive personal information at risk. If for example the counterfoils of cancelled invoices are disposed of in an irresponsible manner, it can pose a risk. The invoice contains customer detail and the link can very easily be made between customer and company.
- Banning certain types of technologies that are outdated will also yield positive benefits, as the audit will identify these types of technologies. Web browsers and data architecture with outdated coding pose security risks as it can be susceptible to attacks (Agre 1997: 24). The same applies to old micro-fiche storage formats that can be stored securely but once the films are accessed and the data is printed, it becomes extremely vulnerable to disclosure. This is especially applicable where there are no clear procedures in place for destroying the printouts in a proper way.

5.2.1 Vulnerability audit

The *vulnerability audit* determines the *internal* and *external* threats that can render one organisation relatively more vulnerable than the next. *Vulnerability* implies the relative weakness that an organisation might possess in terms of a certain area. An organisation with poorly trained employees is much more vulnerable to human error than one with better trained employees. This implies that a specific vulnerability can be rectified. Banks are more susceptible to attacks from criminals who desire the financial details of their customers. If some banks neglect taking proper precautions they become more vulnerable than those banks that did.

Internal threats comprise, amongst other, operational mistakes by *employees*, poorly designed *business processes* or poor *managerial* decision making. *External threats* to privacy can include a host of possibilities:

- *Malicious software,* such as viruses, worms, time/logic bombs and Trojans (Abrams & Podell 1998: 111). Organisations that employ a matrix structure resulting in complicated mail group systems could be very susceptible to worms that replicates by mailing itself in the form of an attachment to every user in the mail group. This eats into the bandwidth of a network and can divulge personal details, such as names, telephone numbers, titles and companies.
- *Crackers* and *programmers* can pose threats as well. Some *programmers* leave 'trapdoors' in the programming code to quickly correct problems but some do it with malicious intent. Malicious programmers who search for these trapdoors could then enter quite easily and gain access and subsequent control (Anderson & Post 2000: 622). *Crackers* are a recurring problem but they comprise a small percentage of the real perpetrators. Mostly people from the inside are responsible for security breaches and data loss (Anderson & Post 2000: 608).
- *Cookies* can pose a threat to a vulnerable organisation (Brinkley & Schell 1998: 17). They are the most common privacy intruders on the web. Important information is stored in the cookie, in its own directory on a PC that acts as an electronic footprint of the user's PC configuration, last site visited and other information (Gupta & Sharma 2002: 8). They create a unique and traceable identity that enables companies to track web surfing patterns and buying patterns, as was the case with Amazon.com (Goldstuck 2002: 8).
- *Competitors* - One of the most important threats is security disclosure of personal information by an authorised person (Abrams & Poddle 1998: 114). The unauthorised deletion or transfer of data is a serious setback and cause systems to work with diminished functionality. Unscrupulous competitors could be interested in causing such a problem in the data of its strongest concurrent.

The following should be included in the vulnerability audit as well:

- **Firstly**, *technological aspects* (hard- and software):
  An organisation should audit its internal procedures to ensure compliance with security and industry compliance standards such as ISO9977, COBIT and ITIL. Where data protection was previously confined to locality, increased processing power brought along the advent of laptops, notebooks and even palm-pads that

are fitted with powerful processing capabilities. They are portable, not confined to locality and able to store huge amounts of information. Web browsing technologies brought along its own challenges and represent enormously complicated pieces of software that are often vulnerable to security compromises.

- **Secondly**, there are the managerial aspects concerning privacy, which include the softer issues concerning the way in which employees interact with the data or the information they access in the course of carrying out their duties. The types of threats and status of employee awareness on privacy will differ from company to company and each company should assess its own exposure to vulnerability.

5.2.2 Data audit

On the analogy of the vulnerability audit, a data audit procedure should be conducted to identify data types that could lead to privacy breaches (Moghe 2003: 69). The audit procedure will identify a) the *risk profile of each data type*, b) *its importance to the company* and the customer as well as c) the *storage, dissemination and disposal thereof.* It also makes good business sense to know your vulnerable areas and to spend at least some amount of money on strengthening these areas.

The following should be covered by the audit:

- Data types with personal and confidential information that are disseminated internally and externally in any form whatsoever. This should even include any type of printable report that might contain any personal information whatsoever.
- It needs to determine if there are any business processes that are insufficient or which is placing the company in possible jeopardy, due to inherent weaknesses in these processes, such as reports with personal information that are thoughtlessly circulated internally or externally or disposed off.
- Determine if any of the current data types and business processes will become redundant in the near future and how this data will be stored or be disposed of when such time arrives. *Old data types* and *disposal policies* are very important. Consider the case of the US Department of Justice who sold outdated equipment to a broker. They did not clean all the hard disks and some contained detailed

information of individuals in their witness protection programs (Anderson & Post, 2000: 610). Micro-fiche film and floppy disks (1.2 Mb-formats) are other prime examples. Universities, hospitals or any other organisation that had to keep signed legal documents on micro-fiche before the introduction of electronic document management systems, are particularly at risk in these areas. These documents contain names, signatures, social security or ID-numbers and other information that can be used for fraudulent activities. Security for this type of technology is confined to locality and extremely difficult and costly to backup. Damage by fire can destroy all these records without any possibility of reconstructing it. An applicable policy and procedure for the continued storage, data type migration or destruction of this data should be in place.

One needs to keep in mind the type of company you are dealing with, as well. Some companies will be more vulnerable, especially if they store huge amounts of data such as is the case with large corporate and governmental databases that are especially at risk (Carnevale & Probst 1997: 250). A manufacturing company with a secure EDI-link to a vendor has a much lower risk and will have a less complex audit procedure, than a company that sells books or items to thousands of people around the world through credit cards, like Amazon.com.

5.2.3 Risk analysis

Once the data audit and the vulnerability audits are completed, the risks are more or less identified and the risk analysis can be conducted. Some additional risks will have to be identified such as loss through fire that will not necessarily be clear from the data or vulnerability audit. Identifying the risk elements is easy enough but calculating their *economic impact* in terms of *magnitude* and *probability* is quite difficult. The *magnitude* and *probability* can be determined by analysing claim patterns in the insurance industry and provides a point of departure for making solid assumptions.

Figure 4 – Risk Analysis

Sample Risk Analysis					
Threat	%-Probability	Loss Range Low	Loss Range High	Weighted Risk Values Low	Weighted Risk Values High
Physical Hazards					
Vandalism	1.5%	R1 000	R2 000 000	R15	R30 000
Software					
Vulnerable legacy systems	50%	R10 000	R100 000	R5 000	R50 000
Anti-virus non-compliance	40%	R15 000	R500 000	R6 000	R200 000
Vulnerable Data Types	60%	R500 000	R1 000 000	R300 000	R600 000
Hardware					
Micro Fiche	10%	R10 000	R50 000	R1 000	R5 000
1.2"-floppy disks	5%	R5 000	R25 000	R250	R1 250
Human Error					
Misaligned Disposal Policy	70%	R350 000	R800 000	R245 000	R560 000
Misaligned Privacy Policy	60%	R200 000	R600 000	R120 000	R360 000
Poor Business Processes	80%	R40 000	R900 000	R32 000	R720 000
Clerical Error	70%	R200 000	R800 000	R140 000	R560 000
			Aggregate Low Value	R849 265	
			Aggregate High Value		R3 086 250

(From Hutt 1995: 1.8)

5.3 Organising

The manager can now commence the organisation process:

- Organise for legal department or persons to assist in the legal framework assessment.
- With the results from the audits and risk analysis known, corrections to weak business processes, vulnerable technology types and data types can commence.
- Communication with all parties about their involvement in the process can commence
- Determination of the policy elements.

The temptation might exist to employ consultants to run the process of the audits, legal framework assessment or any of the other actions to be taken. Although organisations that do not posses an internal pool of expertise might make use of consultants, it remains important that the people within the organisation remain as the owners of the process. The process manager should at all times be in control of what needs to be organised and ensure that he does not only trust the judgement of others that are not as familiar with the industry or organisation.

During the *organising* phase the manager will be able to fully assess the cost implications of the process. It is during this phase that the manager will need to determine the cost of the process. Whilst the audits can be done internally, it can have a cost implication over which the organisation has no control should they choose to make use of external consultants. Correcting the problems identified by the audits though, can be costly and will require frequent and prudent feedback to top management in order to secure their commitment towards providing funds for correcting the problems.

5.3.1 Legal framework assessment

When developing a privacy policy, it should never be a knee-jerk reaction to a legal case (Agranoff 2002a: 4). Proper and continuous assessment must take place to ensure compliance with the legal framework of the home country and that of the other countries where it is conducting its business. Even older legislation is difficult to assess if it is still relevant such as the US Privacy Act of 1974. As with any piece of legislation grappling with relatively new issues, after 30 years, judgement is still out on whether this piece of legislation really succeeded in protecting privacy (Gellman 1997: 193). However the legislation developed, it is always reactive and will always be in a process of evolution due to the ever changing nature of technology and its applications (Mayer-Schönberger 1997: 235).

In assessing the legal framework the following should be kept in mind:

- assessment of all the legal frameworks of different companies within where the company might operate, if applicable and
- consulting legal counsel especially if the company is a multi-national enterprise, as well as
- assessment of previous and relevant cases of privacy breaches and litigation (Erbschloe & Vacca 2001: 61)

5.3.2 Privacy policy elements

Each and every policy should have pre-defined elements that are required to ensure a structured approach to the whole problem. Papazafeiropoulou & Pouloudi (2002: 35, 41) identified six levels at which policy issues should be addressed:

- ***Infrastructure*** –a statement on whether the safest technology possible will be purchased.
- ***Governance*** – Internet expands without government interference and it powerless to control its expansion in any event. It is here that mature governance is required from companies. Especially where legal frameworks are lacking.
- ***Security*** – 30 percent of businesses admitted that they have no security policy in place, despite the sensitive issue of Internet Security and the fact that increased number of computers and transactions increases risk.
- ***Privacy*** – is the information collected over the web used and in some cases sold with the explicit use of the individuals concerned.
- ***Content*** – policy makers on a government level cannot control the content of traffic over the Internet. Organisations should take care about the content of their sales and stipulate in their policies.
- ***Commerce*** – ISO (International Standards Organisation) and the WTO (World Trade Organisation) attempt to standardise global e-commerce as this is important in all EDI-applications. Conformation to these standards, provide the trust element that is often lacking and should be stated in the policy.

The net privacy policy should address the following with relation to how an organisation uses and collects consumer data (Erbschloe & Vacca 2001: 116):

- The policy must state clearly and exactly which types of personal informational items will be collected via the website.
- It must further address the way in which the collected data will be used and whether it will be disclosed to third parties as well as the purpose of the disclosure (Santos 1999: 2).
- If personal and private information is disclosed to third parties, a choice to opt-in, should be provided. Most organisations require an indication to opt-out which implies in actual fact that the disclosure of information to third parties will occur automatically, should the consumer not indicate otherwise. The consumer will therefore be forced to read through the whole policy and will hopefully not read over this particular element in the policy, provided that he is aware of this. This constitutes a huge burden to be carried by the consumer since most of them are not even aware of this. The consumer is already disadvantaged by such a requirement and implies unfair business practice. The burden should move to the organisation where an indication in the policy must be provided to opt-in. Consumers in the EU will find this practice wholly unacceptable. (Santos 1999: 2). Since the EU have the most forward thinking privacy practice, organisations should take note of this, especially in light of the fact that the EU remains South Africa's largest trading partner.
- The use of cookies and whether it will be used to track consumer patterns and attempt link it with real life identities.
- How personal information will be affected when a change in policy occurs. The organisation might change its policy on information disclosure. It must be stated if this will then be applicable to all stored data or only the data collected after the date of change.

5.4 Closure

After the completion of the *audits*, the identification of *privacy policy elements* and the *legal framework assessment*, the initial drafting of the policy can commence and is an important part of the process (Erbschloe & Vacca, 2001 83). This constitutes the completion of the *development phase* and paves the way for *implementation*. This process is never really completed due to constant changes in the legal framework, changing business environment and the invention of the new technologies. In this sense the development of a net privacy policy is, therefore, never complete.

Developing a net privacy policy is an *iterative process* but after the initial first draft, the *implementation phase* must commence. The process must move forward and there will be sufficient opportunities in the *communication* process, a vital part of the *leading function*, to make additions and changes. The next chapter will investigate the *implementation phase*.

Chapter 6: Privacy policy implementation phase

Synopsis

The *implementation phase* in a sense is more difficult to execute. During this phase the *management functions* of *leading* and *controlling* will ultimately have to deliver the desired outcomes as set out in the beginning. The *leading* very much concerns the softer issues where *training* and *communication* takes place. It is not always that easy to make each and everyone within the organisation aware of all the related issues.

The function of *controlling* is extremely difficult to execute. It is through this function that the manager can determine the success of the process and the policy. If there is no litigation or problems arising, due to a well designed policy and implemented, it could be argued that too much time and money was spent on the whole process. If on the other hand, however, some serious problems do arise due to a poorly constructed policy or for any other reason, the organisation will feel that its efforts were inadequate.

6 Privacy policy implementation phase

6.1 Introduction

At this stage, the policy will have been drafted and revised several times. At a stage where all the parties are satisfied with the content, it can be implemented. At this stage, the parts of the net privacy policy that directly impacts on the users visiting the organisation's website can be published in the form of a *privacy statement*.

Implementation of the accepted policy should occur right through the organisation through proper guidelines, procedures and through the involvement of different departments (Agranoff 2002a: 12). To co-ordinate this effort, it is advisable to employ a *project plan* to manage the process. The *project plan* can be designed in the development and planning phase but its importance increases in the *implementation phase*, since the deliverables of the process will become more apparent.

6.2 Leading

Leading does not require the same amount of preparation as in the case of *planning* and *organising* but it is a very important phase within the process with its own challenges. Proper leadership or the lack thereof will determine the success or failure of the process.

- The manager charged with the responsibility of the privacy policy cannot possess all the knowledge and skills needed to conduct a process that is in essence a multi-disciplinary one. The *co-operation* of all departments, including Human Resources, Information Technology, Legal and any other advice that is relevant should be obtained (Agranoff 2002a: 12). The ability to recruit and mobilise people for a cause is therefore important.

- *Co-operation* can only be achieved through *communication* to, and *training* of employees and other managers. If the communication process breaks down, the importance of privacy protection will not be imposed on all employees.

Although most of the preparation will have been completed during the development phase, the leading function will put the issues identified in place. The leadership responsibility becomes important when the weaknesses identified must be rectified through action.

6.2.1 Communication

The privacy manager will now have to consult with the IT-manager on how to strengthen or migrate vulnerable data types and technologies. He will have to consult with all departments that are employing business processes that can jeopardise personal information. Some business processes run across several departments and the management challenge in this regard becomes much more acute. This requires a communication process and structures to be in place for it to be successful.

It is important that communication on an internal level receive adequate attention in the form of an internal awareness campaign and in some instances an external awareness campaign should also be conducted (Erbschloe & Vacca, 2001 109). This will be directed towards customers especially but also to suppliers, strategic partners and vendors.

6.2.2 Training

Training employees and managers on all levels is extremely important (Moghe 2003: 68) and should start with the executive management so that the message can filter down to the lower levels. Erbschloe & Vacca (2001: 103) determined three types of training during the process namely 1) *executive level*, 2) *middle management* and 3) *supervisors*. There are also the *project leaders who are* responsible for the project

leadership who should receive training as well. Depending on the type of organisation, the human resources profile and educational levels of employees, it might also be necessary to train employees on *operational level*. These can include data capturers and administrative staff, that most often have more access than one would care to admit at first.

It is surprising how many companies disclose clients' personal information contrary to their own privacy policies and then having management even admitting to it (Proquest 2004b: 2). There are also examples of top management banking officials admitting to the fact that they are not sure whether their websites even need privacy statements where these banks engage in e-commerce (Wade 2004: 19). This illustrates the need for training on all levels based on the assumption that if training has a positive effect on top management, they would buy in to the idea of privacy management and enforce the issue down to all levels of the organisation.

6.3 Controlling

The insufficient attention that is given to the controlling function was already noted (4.2). Structures should therefore be in place to *manage* and *monitor* the success of the process conducted. The technological environment and legal framework is ever changing and continuous assessment will be required (Erbschloe & Vacca 2001: 141). This also implies that continuous *training* and *communication* will have to be in place to inform all levels of the organisation of any changes that might immediately affect them or their activities.

Each organisation will have to determine at what intervals they need to redevelop or revise their policies. This will include amongst other things, the way that technology is managed. *Firewalls* and *encryption* are still in use to provide security (Erbschloe & Vacca 2001: 199). New technological developments and their implications for privacy must also be assessed on a continuous basis. Most *ERP-systems* have *web browser technologies* that allow employees to *telecommute*. Working from home has its benefits to the company and the employees but the home environment cannot be

controlled. Sessions left running and unattended at home could put the organisation at serious risk, depending on the type of employees and the sensitivity of the data they are entrusted with.

Remote access is another problem where employees are working from hotel rooms or other sites and pose many risks to the organisation (Erbschloe & Vacca 2001: 270). Employees can download all kinds of harmful programs during office hours, from the Internet, using a web browser which vulnerabilities are not properly known. This web browser might be susceptible to attacks where an attacker can gain control over the user's computer or run a malicious code of his own. Attacks through web browsers occurred as early as 1997, such as the Macromedia Shockwave problem (Garfinkel & Spafford 1997: 72) but even today there are various vulnerabilities exposed in the components of the Windows operating system where attackers can gain control over a user's computer through web browsers or related components (Microsoft 2003: Internet). Even a simple decision like installing a new web browser can, therefore, create a security risk to privacy. It is important that technology be monitored on an on-going basis and that an integrated communication channel is established between the privacy manager and the IT-manager in this instance.

In other countries, new privacy legislation challenged the way they used their technology. Some organisations struggle to come to terms with constant changes in privacy legislation and alignment and it is even necessary to engage in in-house developments of software to accommodate these changes that has a huge cost implication (Moghe 2000: 63).

6.3.1 Determine the effects of the process

It is difficult to determine the effect of the net privacy policy-making process. In the event of a company that experienced frequent privacy breaches, it becomes more measurable since the number of breaches can be calculated. In some instances, however, it will resemble the preparation for the Y2K-vulnerability. Long after organisations are still unsure about how well spent efforts were that companies had

to undergo to ensure Y-2-K-compliance. Its value can only be determined in the long run and sometimes even if there are no occurrences which makes it difficult to sell the importance of such an effort to management. It is therefore important that a relationship of trust is built with the consumers visiting the website of organisations. A lack of trust is one of the greatest barriers to e-commerce growth and the situation is aggravated by the constant bombardment of consumers with unsolicited e-mail, spam, pornography and privacy breaches (Peeples 2002: 28-31).

A very important aspect is the *iterative nature* of privacy management. The ever changing *legal* and *technological environments* were noted above. This requires continuous assessment and implies that the work of the privacy manager is never finished. Attitudes, ideas and the thinking of people within the organisation change constantly as well. The media and their own inter-action with others determine their attitudes and behaviour towards privacy. The issue becomes even more complex when one considers the impact that a changing privacy policy can have on the other policies noted in Figure 1.

6.4 Closure

Leading and providing leadership during this phase is not always easy to quantify as the efforts, *communication* and people skills of the manager will ultimately determine the success or failure thereof. Establishing a *communication* network and a *training* structure are therefore meant to support this function and avoiding its degradation into a blurred and unstructured effort.

Revisions will have to be accepted as the awareness of privacy will increase and responsible managers will discover more of the implications than they could muster with their initial efforts. The *controlling function* will provide a structured treatment of the iterations needed to build an ironclad policy and to determine the success of the process. This once again demonstrates the *iterative nature* of *developing* and *implementing* a *net privacy policy*.

Chapter 7: Final and summary remarks

Synopsis

The final chapter contains concluding remarks based on the results of this study. It presents a brief overview of the research objectives and its results. This chapter also provide a synopsis of the study, providing an accessible and readable overview. The closing remarks at the end of this chapter, provides even more motivation for instating privacy protection initiatives within an organisation by looking at the current state of privacy protection in South Africa.

7 Final and summary remarks

7.1 Introduction

The problematic issues surrounding privacy are often misunderstood because privacy does not succeed in capturing the same amount of attention as does other issues such as energy and the environment (Ware 1979: 10) and most organisations only realise the dangers, once it is too late. This is disconcerting since privacy concerns have been around for a long time. George Orwell had visions of 'Big Brother' in 1948 and Aldous Huxley wrote in 1931 about his own visions of 'A Brave New World' where privacy was under threat by technological developments (Agranoff 2002b: 41).

The nineties saw the advent of Web Browser Technologies and e-commerce in the form of b-2-b and b-2-c transactions. Since personal information must be disclosed to effect these transactions, privacy changed from a political and social rights issue (Steel 1979: 4) of the seventies to a consumer-rights issue in the late nineties (Davies 1997: 143). Consumers claim the right to privacy of their personal information. They pay for services or goods with money as the final form of payment. They do not barter their privacy for the services or products bought. The modern concerns are the same as those of more than seventy years ago:

- Consumers want to know who holds their personal information. They want to be assured that the gatekeepers entrusted with this task can be relied upon.
- Consumers are concerned about the way their personal information is disseminated throughout the organisation and they way it is used.
- They want to know who has access to their personal information, such as third parties, or plainly stated: Who else knows who we are?

The concerns do not affect the consumers alone but organisations as well:

- Consumers and people in general fear that the loss of private information can result in financial loss or victimisation where sensitive private information is

disclosed such as HIV-status. Theft of identity or other details can result in serious financial loss. One only needs to be reminded of the resent spate of media reports where a leading South African bank's customers were defrauded out of thousands of rands (Opperman 2003b, 16).

- The negligent management of privacy can lead to serious financial loss and a tarnished public image. DoubleClick Inc. lost 20% of its market value in two months due to a callous attitude towards consumers' right to privacy by tracking their web surfing patterns through cookie information. Only after immense public and political pressure, they seized their actions (Erbschloe & Vacca 2001: 16).

It is therefore in the interest of society and business alike to protect privacy.

7.2 Privacy issues

Organisations must learn to understand and deal with the listed issues and concerns of consumers in order to avoid the unfortunate examples above. Privacy issues are complex and require well-informed managers, with multi-disciplinary backgrounds to deal with it. First and foremost, organisations need a *privacy definition* to adequately deal with these diverse and wide ranging issues. Reaching such a definition is not an easy task and can differ from country to country in legal and customary terms. It can have far reaching implications for multi-national companies because the understanding of privacy as well as the legal framework can differ in every country in which such an organisation has business interests.

Discerning between *privacy* and *net privacy* with regard to the underlying differences is equally difficult. Almost all companies today have *privacy statements* posted on their websites to inform all visitors of how their personal detail gathered from the website will be disclosed. A net *privacy policy* is far more encompassing than a *privacy statement* and will determine all related policies with regard to:

- Disposal of assets policies where care should be taken how old computers and the information (collected through the Internet) they store are disposed of.

- Access to information policy – determining the boundaries of access up to the point where it infringes on the rights of privacy.
- E-mail policy for employees.
- Internet access policy.
- Employee surveillance policy.

The *legal framework* in which an organisation operates can be the single most complex privacy issue to deal with. The reasons are as follows:

- Some companies operate in more than one legal framework if they are multi-nationals.
- The legal framework changes constantly and is determined by a dynamic environment where the judgement of a court can change the course of legal interpretation (Holvast 1993: 269).
- Organisations must subsequently continually assess the legal framework(s) in which they operate.

Technology also develops constantly. New applications for existing technology develop continuously, together with the rapid development of new technologies. Observers, activists and even ordinary people viewed technological development with a sense of suspicion, since they feel that it is threatening towards their privacy (Holvast 1993: 272). It is therefore important that organisations manage and understand *privacy issues* and realise that it makes good business sense to deal with the different dimensions of privacy in one's industry. By doing this, organisations can avoid costly litigation, bad publicity and gain the trust of consumers in the process that will ultimately lead to the desired increase in e-commerce transactions (Carroll 2002: 51).

7.3 Management challenges

The *privacy issues* that were identified above create the *management challenge* – how does a manager succeed in balancing all parties' interests by managing these issues for the benefit of the organisation and its customers? The *management*

challenge is embedded in the successfully managed process that turns *privacy issues* into a competitive advantage:

- Managing and understanding *privacy issues* on all levels of the organisation so that the above mentioned examples of organisations that neglected privacy issues can be avoided.
- Managing privacy issues requires an understanding of the related *risks* and probabilities unique to the industry and organisation.
- How to meet the challenge of managing *people* and their interaction with *technology* that can create possible privacy breaches.
- Manage effectively so that business is conducted in an ethical manner and embedding trust in e-commerce websites that can lead to a growth in e-commerce since the lack of trust in these websites has thus far inhibited the growth of e-commerce. This in turn will secure *customer satisfaction* and in the process create a *competitive advantage* (Santos 2000: 1).

The private information of individuals within an organisation's database should not be breached or disclosed. This represents a *risk*. Managers need to determine the cost and probability of this *risk* and put measures, policies and procedures in place to avoid this from happening. In other words, the *risk* must be managed in a proper way by conducting a proper *risk analysis* in a responsible manner that rests on a solid rational base. This can include the building of a *technical* and a *legal hedge*. Providing a secure *technical* and *legal hedge* is extremely important but it is not enough. Although it represents one side of the coin, the human factor must be accounted for since it represents the biggest risk factor (Holvast 1993: 273).

A huge responsibility rests on management to secure private information by putting measures and policies in place to protect it (Zakin 1995: 2.3-2.5). Apart from the overall framework that managers have to put in place for the protection of privacy, they need to make decisions that seem simple. Some organisations require visitors to their websites to opt-out if they do not want to receive promotional material. The responsible management approach should be a more ethical one by requiring visitors to rather opt-in for mail and promotions.

7.4 Determining a management approach

In order to address the above *management challenges* management should select a management approach that is applicable to unique privacy problems.

- *Flexible* to be applicable to almost all situations where privacy issues are managed and must be able integrate the various fields and disciplines.
- It must be a *generic process* to ensure the required *flexibility*.
- It must be of a *multi-disciplinary* nature to incorporate all legal, human and customer related issues as identified in the previous chapter and should take cognisance of project management elements as some wide-ranging (multi) disciplines need to be incorporated into the process.
- It is an *iterative process* due to the ever-changing global, technological and legal environments. Continuous assessment is therefore necessary with every legal change or perceived change in consumer or employee attitudes.
- The *involvement* of *employees* as well as the *support of top management* is essential and it stands to reason that it must be accounted for in the process. Employees will ultimately be responsible for enforcing the net privacy policy. They must respect the policy and its contents. It is just not good enough for management to understand all the issues. The employees in operational units are crucial links in the process. It is at operational level, where the privacy breach can occur.

The *implementation* and *development* of a net privacy policy is a managerial function governed by the four *basic management functions* of *planning*, *organising*, *leading* and *controlling*. These are the generic functions found in all management processes. Due to the *multi-disciplinary* nature of privacy management, a project management approach must be implemented to drive these basic management functions. Planning and organising will make up the development phase and will be followed by leading and controlling functions that will make up the implementation phase. This project management approach differs from most other due to the fact that it is an on-going effort that is never really completed. This is due to the ever changing legal and

technological environments that require constant monitoring and reworking. Once an organisation followed this approach to establish its initial privacy policy, it must constantly train employees, adjust their attitudes, modify the policy to make provision for new technological and legal developments. The process is therefore *iterative*.

7.5 Developing and implementing a net privacy policy

The planning and organising functions make up the development phase where the following important actions should be taken:

- *Vulnerability audit* to determine how vulnerable the organisation is to privacy breaches in terms of its business processes, industry, technologies employed and any other relevant aspect.
- *Data audit* to determine and identify vulnerable data types such as old storage formats, poor procedures, disposal policies relating to data storage and paper reports to name but a few.
- *Risk analysis* to determine the probability of risks involved as well as low and high levels of each. The costs are determined by the minimum and maximum claims to insurance companies and other relevant determinants such as recovery costs.

Once the above are known, the manager knows what to plan and organise for. *Organising* can now commence to assemble resources and determine the scope of the project. During this phase, the *legal framework* can be assessed and the privacy *policy elements* can be determined.

The *implementation phase* is of equal importance and is made up of the *leading* and *controlling* functions. Central to the leading function is a *communication* process where information is disseminated throughout every level of the organisation. This serves the following purpose:

- Ensure adherence to the project plan.
- Compliance with the principles and objectives of the processes.
- Create familiarity with the privacy issues.
- To co-ordinate the multi-disciplinary effort successfully.

This does not imply however that the communication process only start at this stage of the whole process. It stands to reason that it should be present at all times. This stage of the management process however requires solid communication to report on the progress, identify problems and inform all the role players contributing of the process.

Apart from the communication, *training* is an essential part of the leadership function. Managers cannot provide leadership to employees if they are not familiarised with or sensitised to privacy issues. *Training*, like communication will have to be conducted long after the management process has been completed. The reasons are simple and are due in part to the changing legal and technological environment that impact on the attitudes and behaviour of an organisation's employees.

Workshops and information sessions are too often reserved for managers. Effort and care should be taken to especially involve lower level employees such as those on operational level who actually are in daily contact with situations that can develop into privacy breaches. Top management should also not be neglected in receiving training or information. As long as top management believes in the importance of privacy protection and its benefits to the organisation and its customers, privacy protection will be a priority.

The *controlling* function is surely the most neglected function in all management processes. Admittedly, it is difficult to determine the success of such an effort. If a breach never occurs some employees, including management, might wonder if it was worth all the effort. It might never occur to them that there are no privacy breaches because the process was properly conducted. When a privacy breach does occur, it can cast the project in doubt as well. An important facet of the *controlling* function is the iterative nature of the management process. Once the management process is laid down and a policy constructed, constant evaluation and monitoring of the legal, technological and other environments are necessary to protect the organisation, its employees and the private information of their customers.

The importance of the iterative process in the *controlling phase* is underscored by the fact that compliance levels to the ECT-Act dropped by 30%. A survey by the IT attorney firm, Buys Inc., found that as much 81% of Websites in South Africa did not comply with provisions of the ECT-Act of 2002. Almost two years after the passing of the act, most companies do not comply and only one company (TELKOM) demonstrated 100% compliance. The use of privacy policies dropped from 15% to 8% as well as an absence of proper disclaimers. The results could be damaging because non-compliance invites a range of legal liabilities, including civil liability, criminal fines, copyright infringement, trademark abuse, repudiation of contracts and investigation by the Consumer Affairs Committee (Burrows 2004: 1).

One of the reasons given by companies for not complying was due to the high cost of contracting consultants. Organisations must be prepared to allocate expenditure for privacy compliance and realise that once the privacy policy is finished, a lot of work still remain. The project must be conducted on an ongoing basis so as to avoid the possible damaging results mentioned above. It is in the interest of society at large and business to protect privacy.

Bibliography

ABRAMS DA & PODELL HJ. 1998. Malicious software (*In* Marshall DA, Jajodia S, Podell HJ *eds.* Information security: An integrated collection of essays. Los Alimos, California: IEEE Computer Society Press. pp 111 – 126.)

AGRANOFF MH. 2002a. E-Mail: Balancing corporate assets and employee privacy. (*In* Herold R *ed.* The privacy papers: Managing technology, consumer, employee and legislative actions. Boca Raton, Florida: CRC Press LLC - Auerbach Publications. pp 3-14.)

AGRANOFF MH. 2002b. Policies for secure personal data. (*In* Herold R *ed.* The privacy papers: Managing technology, consumer, employee and legislative actions. Boca Raton, Florida: CRC Press LLC - Auerbach Publications. pp 41-50.)

AGRE PE. 1997. Beyond the mirror world: Privacy and the representational practices of computing. (*In* Agre PE & Rotenberg M *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 29-62.)

ANDERSON DL & POST GV. 2000. Management information systems: Solving business problems with technology. 2nd ed. Burr-Ridge, Illinois: Irwin/McGraw-Hill. 665 pp.

BATEMAN T & SNELL S. 1999. Management: Building competitive advantage. 4th ed. Boston Burr-Ridge, Illinois: Irwin/McGraw-Hill. 642 pp.

BELOTTI V. 1997. Design for privacy in multimedia computing and communications environments. (*In* Agre PE & Rotenberg M *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 63-98.)

BENNET CJ. 1997. Convergence revisited: Toward a global policy for the protection of personal data? (*In* Agre PE & Rotenberg M *eds.* Technology and Privacy: The New Landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 99-124.)

BIGELOW RP. 1995. Legal issues in computer security. (*In* Hutt EA, Bosworth S & Hoyt DB *eds.* Computer security handbook. 3rd ed. Somerset, New Jersey: J Wiley. pp 5.1-5.29.)

BOLOGNA GJ. 1995. Computer crime and computer criminals. (*In* Hutt EA, Bosworth S & Hoyt DB *eds.* Computer security handbook. 3rd ed. Somerset, New Jersey: J Wiley. pp 6.1-6.31.)

BRINKLEY DL & SCHELL RR. 1998. What is there to worry about? An introduction to the computer security problem. (*In* Marshall DA, Jajodia S & Podell HJ *eds.* Information security: An integrated collection of essays. Los Alimos, California: IEEE Computer Society Press. pp 11-40.)

BURROWS T. 2004. SA sites don't comply with ECT Act. IT-Web. September 20. [Web: http://www.itweb.co.za/sections/internet/2004/0409201028.asp?S=Legal%20View&A=LEG&O=FRGN#contacts Date of use: 15 Oct. 2004].

CAPUDER LFM. 2002. Developing an organisational internet policy. (*In* Herold R *ed.* The privacy papers: Managing technology, consumer, employee and legislative actions. Boca Raton, Florida: CRC Press LLC - Auerbach Publications. pp 23-32.)

CARNEVALE PJ & PROBST TM. 1997. Conflict on the Internet. (*In* Kiesler S *ed.* The culture of the Internet. Mahwah, New Jersey: Lawrence Eribaum Associates, Publishers. pp 233-255.)

CARROLL B. 2002. Price of privacy: Selling consumer databases in bankruptcy. *Journal of interactive marketing.* 16(3) pp 47-58. Summer.

COOPER, DR & SCHINDLER PS. 2001. Business research methods. 7th ed. New York: McGraw-Hill. 798 pp.

CORBY JM. 2002. The case for privacy. (*In* Herold R *ed.* The Privacy Papers: Managing technology, consumer, employee and legislative actions. Boca Raton, Florida: CRC Press LLC - Auerbach Publications. pp 3-14.)

DAVIES SG. 1997. Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity. (*In* Agre PE & Rotenberg M. *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 143-166.

DREYER LCJ. 1999. The InfoPriv model for information privacy. Johannesburg: RAU. (Informatics Thesis – PhD). 162 pp.

ERBSCHLOE M & VACCA J. 2001. Net privacy. New York: McGraw-Hill. 318 pp.

GARFINKEL S & SPAFFORD G. 1997. Web security & commerce. Cambridge: O'Reilly & Associates Inc. 483 pp.

GELLMAN R. 1997. Does privacy law work? (*In* Agre PE & Rotenberg M *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 193-218.

GIBSON JL, IVANCEVICH JM & DONNELY JH. 2000. Organizations: Behaviour structure processes. 10th ed. Burr-Ridge, Illinois: Irwin McGraw-Hill. 522 pp.

GOLDSTUCK A. 2002. "By their readings ye shall know them." *The Future:* April.

GRIFFIN MT, BELANGER F & VAN SLYKE C. 2002. Multi-dimensional b2b auctions for electronic commerce. (*In* Fazlollahi B *ed.* Strategies for ecommerce success. Hershey, Pennsylvania: IRM Press. pp 271-277.)

GUPTA JND & SHARMA SK. 2002. Cyber-shopping and privacy. (*In* Fazlollahi B *ed.* Strategies for ecommerce success. Hershey, Pennsylvania: IRM Press. pp 2-16.)

HITT MA, IRELAND RD & HOSKISSON RE. 2001. Strategic management: Competitiveness and globalization. 4th ed. Cincinnati, Ohio: South-Western College Publishing. 1142 pp.

HOLVAST J. 1993. Vulnerability and privacy: Are we on the way to a risk-free society? (*In* Berleur J, Beardon C & Aufer R *eds.* Proceedings of the IFIP WG9.2 (International Federation for Information Processing Transactions) Working conference on facing the challenge of risk and vulnerability in an information society. Amsterdam, Netherlands: Elsevier Publishers. pp 267-277.)

HUTT AE. 1995. Management's role in computer security. (*In* Hutt EA, Bosworth S & Hoyt DB *eds.* Computer security handbook. 3rd ed. Somerset, New Jersey: J Wiley. pp 1.1-1.37.)

KOTLER P. 2000. Marketing management. Upper Saddle River, New Jersey: Prentice-Hall. 718 pp.

LAWS *see* SOUTH AFRICA.

LOTRIET D. 2002. Easyinfo nie jammer oor akkurate inligting. *Rapport*. Maart 17.

MAYER-SCHÖNBERGER L. 1997. Generational development of data protection in Europe. (*In* Agre PE & Rotenberg M *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 219-242.)

MEREDITH JR & MANTEL SJ. 2000. Project management: A managerial approach. 4th ed. Toronto: John Wiley. 616 pp.

MICROSOFT CORPORATION. 2003. Security Update, May 09, 2003 (updated) (MSXML 4.0). [Web: http://www.microsoft.com/technet/security/bulletin/MS02-008.mspx Date of use: 4 Jun. 2004].

MILLER AR. 1971. Assault on privacy: computers, data banks and dossiers. Michigan: The University of Michigan Press. 331 pp.

MOGHE V. 2003. Privacy management - a new era in the Australian business environment. *Information management & computer security*, 11(2). [In EMERALD: Academic Full Display: http://emeraldinsight.com.raulib.rau.ac/ Date of use: 7 Apr. 2004].

OBERHOLZER HJG. 2001. A privacy protection model to support personal privacy in relational databases. Johannesburg: RAU. (Informatics Dissertation – M.Sc.) 135 pp.

OPPERMAN H. 2003a. ABSA-'kraker' steel kliënt-inligting ID-kodes vooraf van kliënte verkry deur e-pos-boodskap. *Sake-Beeld*. Julie 21.

OPPERMAN H. 2003b. ABSA verduidelik kraker-probleem. *Beeld, Verbruikersforum*. Augustus 25.

PAPAZAFEIROPOULOU A & POULOUDI A. 2002. Social issues in electronic commerce: Implications for policy makers. (*In* Fazlollahi B *ed.* Strategies for eCommerce success. Hershey, Pennsylvania: IRM Press. pp 32-49.)

PEEPLES DK. 2002. Instilling consumer confidence in e-commerce, 67(4). *S.A.M. Advanced Management Journal*, (5 p.), Autumn. [In PROQUEST: Academic Full Display: http://0-proquest.umi.com.raulib.rau.ac.za/ Date of use: 25 Mar. 2004].

PHILLIPS DJ. 1997. Cryptography, secrets and the structuring of trust. (*In* Agre PE & Rotenberg M *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 243-276.)

PROQUEST. 2004a. Corporate privacy policy respecting the collection, use and disclosure of personal information. *Canadian Medical Association Journal.* 170(1), January 6. [In PROQUEST: Academic Full Display: http://0-proquest.umi.com.raulib.rau.ac.za/ Date of use: 6 Apr. 2004].

PROQUEST. 2004b. Airlines provide passenger information. *The New American.* 20(3), February 9. [In PROQUEST: Academic Full Display: http://0-proquest.umi.com.raulib.rau.ac.za/ Date of use: 6 Apr. 2004].

SAKEBEELD. 2003. Data op ou rekenaars kan probleme skep. September 23.

SAMARAJIVA R. 1997. Interactivity: As though privacy mattered. (*In* Agre PE & Rotenberg M *eds.* Technology and privacy: The new landscape. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press. pp 277-310.)

SANTOS J. 1999. Two views of data protection: EU versus US. META Group, Inc. Executive Directions. [Web: http://www.metagroup.com Date of use: 1 Dec. 2003].

SANTOS J. 2000. Privacy matters. META Group, Inc. Executive Directions. [Web: http://www.metagroup.com Date of use: 1 Dec. 2003].

SOUTH AFRICA. 1996. Constitution of the Republic of South Africa 1996 - As adopted on 8 May 1996 and amended on 11 October 1996 by the Constitutional Assembly. Act 108 of 1996. (ISBN 0-620-20214-9). [Web: http://www.polity.org.za/html/govdocs/constitution/saconst.html Date of use: 4 Jun 2004].

SOUTH AFRICA. 1998. Open Democracy Bill, no 67. [Web: http://www.polity.org.za/html/govdocs/bills/1998/index.html Date of use: 4 Jun 2004].

SOUTH AFRICA. 2000. Promotion of Use to Information Act, no 2. [Web: http://www.polity.org.za/html/govdocs/legislation/2000/index.html Date of use: 4 Jun 2004].

SOUTH AFRICA. 2002. Electronic Communications and Transactions (ECT) Act, no 25. [Web: http://www.polity.org.za/pol/acts/2002/ Date of use: 4 Jun 2004].

STAMPER DA. 1994. Business data communications. 4th ed. Redwood City, California: The Benjamin Cummings Publishing Company, Inc. 608 pp.

STEEL D. 1979. Information privacy: An overview. (*In* Hewitt P *ed.* Computers records and the right to privacy (National Council for Civil Liberties)). United Kingdom, Surrey: Input Two-Nine Ltd. pp 1-8.)

TOMLUK D & PINSONNEAULT A. 2002. Customer loyalty and electronic banking. (*In* Fazlollahi B *ed.* Strategies for eCommerce success. Hershey, Pennsylvania: IRM Press. pp 89-109.)

VINAJA R. 2002. Mobile agents, mobile computing and mobile users in global e-commerce. (*In* Fazlollahi B *ed.* Strategies for eCommerce success. Hershey, Pennsylvania: IRM Press. pp 278-288.)

WADE W. 2004. Banks slow to answer web queries. *American Banker*, 196(17), (3 p.), January 26. [In PROQUEST: Academic Full Display: http://0-proquest.umi.com.raulib.rau.ac.za/ Date of use: 25 Mar. 2004].

WARE WH. 1979. Privacy and information technology – The years ahead. (*In* Hoffman LJ *ed.* Computers and privacy in the next decade. Pacific Grove, California: Academic Press. pp 9-22.)

WITTAKER S & SIDNER C. 1997. Email overload: Exploring personal information management of email (*In* Kiesler S *ed.* The culture of the Internet. Mahwah, New Jersey: Lawrence Erbaum Associates Publishers. pp 277-295.)

ZAKIN NK. 1995. Policies, standards and procedures. (*In* Hutt EA, Bosworth S & Hoyt DB *eds.* Computer security handbook. 3rd ed. Somerset, New Jersey: J Wiley. pp 2.1-2.30.)