THE PROTECTION OF COMMERCIAL INFORMATION IN ELECTRONIC COMMUNICATIONS WITH SPECIAL REFERENCE TO THE INTERNET

By

Leani Marlie van Schalkwyk

Submitted in accordance with the requirements for the degree

MAGISTER LEGUM

In the

Faculty of Law
Department of Mercantile Law

of the

University of the Free State
BLOEMFONTEIN

Supervisor:
Prof. J.J. Henning

November 2003

Quis custodiet ipsos custodes?

- Juvenal

I declare that the dissertation hereby submitted by me for the LL.M degree at the University of the Free State is my own independent work and has not previously been submitted by me at another University/faculty. I furthermore cede copyright of the dissertation in favour of the University of the Free State.

_____

LM VAN SCHALKWYK

TABLE OF CONTENTS

PAGE

CHAPTER THREE

PERSONAL ELECTRONIC DATA PROTECTION: UNITED STATES

CHAPTER FOUR

PERSONAL ELECTRONIC DATA PROTECTION: EUROPE

CHAPTER FIVE

PERSONAL ELECTRONIC DATA PROTECTION: **SOUTH AFRICA**

CHAPTER SIX

PERSONAL ELECTRONIC DATA PROTECTION: **UN GUIDELINES AND OTHER DOCUMENTS**

CHAPTER SEVEN
CONCLUSION AND RECOMMENDATIONS

CHAPTER ONE
INTRODUCTION

1. General Introduction[1]

The era in which we find ourselves demonstrates the rapid development of technology. Information that would have been practically inaccessible a few years ago is available to anyone with a computer or Internet[2] access. In the beginning of the previous century everybody's personal papers and details were kept in their houses and places of business. Today this detailed information is on computer disks. It is in most instances not even in our possession but is in the custody of third parties – banks, insurance companies, medical institutions and employers, to only name a few.

With the progress associated with technology and the information industry, life has become much more convenient. Banks claim that a person can do his or her necessary banking in front of the computer at any convenient time. Online shops and merchants lure "shoppers" into the magical world of cyber malls where you can purchase anything your heart desires without leaving the comfort of your own home.

This accessibility to innumerable opportunities can pose a danger to the individual. The darker side of progress has many times been coined as an involuntary sacrifice of privacy and the peace of mind that your interests are safe.

Information is constantly being gathered, filtered and processed for different purposes. How can a person ensure that information that was intended not to be freely available is not publicised?

The green paper on e-commerce[3] worded this dilemma quite clearly: "Privacy or the lack thereof, is a major concern for individuals in the use of the electronic medium in commerce. This includes not only the privacy of the communication between the parties

[1] Because of the technical nature of this study a list of relevant definitions and terms is supplied at the end of this dissertation in the form of a list of key terms for purposes of reference.
[2] See page 120 for a list of key terms.
[3] See chapter 3 (3.1)

in a transaction e.g. the protection of credit and debit card numbers while traversing the Internet, or of other personal details, which can be solved through the use of encryption; but also the accumulation of personal data at web sites[4] visited, for example through the use of “cookies”[5]

The Internet has changed the way people interact and communicate, and has created a new “community” for businesses, academics, and others. Because of the borderless nature of the Internet, ordinary legal paradigms do not always apply and moral and legal structures break down in cyberspace.[6] As more information becomes available over the Internet, that information is increasingly more vulnerable since it includes increasing volumes of commercial and personal information.

1.1 Scope and Purpose of the study

In protecting information, the interests of its proprietor or holder, as well as the interests of the person(s) "owning" the information, or data subject, must be protected.

The question pertaining to the protection of information of the person concerned (the subject of the information) has an inescapable connection with the aspect of privacy. The principle of privacy is an age-old discussion with legions of facets. The seemingly simple task to formulate a definition and to explain this concept proves to be overwhelming. However, it is not the purpose of this dissertation to study the principles of privacy or try to achieve the above-mentioned task. With this in mind a basis needs to be set from which to depart.

The desire for privacy is an elementary human need that has manifested itself as part of national law through the ages. This right is expressed as a fundamental human right in the South African Constitution.[7] The right to privacy is guaranteed expressly in the Universal Declaration of Human Rights,[8] the European Convention on Human Rights,[9]

[4] For a definition of “Web site” see page 120 in the list of key terms.
[5] See chapter 2 (2.1.2) and page 120 in the list of key terms.
[6] For a definition of “cyberspace” see page 120 in the list of key terms.
[7] In section 14 of the Constitution of South Africa this right is worded as part of the Bill of Rights.
[8] Article 12
[9] Article 8

the International Covenant on Civil and Political Rights[10], the American Convention on Human Rights.[11]

One must draw a distinction between privacy in the widest sense and *information* privacy as a particular aspect thereof. This narrows the scope of the study since it incorporates the principle that other people should not obtain knowledge about one without one's consent.[12] In this sense the definition supplied by Westin is satisfactory: "['Information privacy' is] the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[13]

The aspect of information privacy will form the basis of the privacy part of the study, which also represents an area which is frequently threatened by the development of information technology. To further refine the relevant scope it should be pointed out that the wide area of information technology (IT) is reduced to concentrate on aspects concerning the Internet.[14]

To determine how commercial information can be protected, it must be ascertained whether protection provided by privacy principles is adequate or whether further protection is needed.

The interests of the holder or proprietor of information should also be considered. This person can be the subject of the information or another person or entity that has been entrusted with information, which, in most cases is of a confidential nature.

The study is divided into two parts. Attention is given to the aspect of cybercrime with special reference to cybercrime that concerns information. It is also investigated whether sufficient protection is conferred to the holder of data.[15] This will form the first part of the dissertation and also represent a horizontal type of data protection among

[10] Article 17
[11] Article 11
[12] Michael 1994:6
[13] Westin 1968:7
[14] Telephones, cellular phones and other electronic means of communication does not in essence form part of This dissertation and may be mentioned only as illustration.
[15] The words "data" and "information" is used interchangeably in this dissertation and no semantic distinction is made between the two terms.

peers or individuals mutually. This horizontal "relationship" is derived from the fact that protection is granted to an individual because of the threat of interception of data by other people (not governmental bodies), irrespective of the fact that criminal law is involved. The question whether common law principles apply to information crime[16] that is committed over the Internet, is also touched upon.

The second part deals with the privacy aspect and specifically the protection of the interests of the person concerned (the subject of the information). This part concentrates on a vertical type of relationship since this part includes the protection of personal data by data controllers, who, in most instances, are types of organisations, government agencies or businesses that operate over the Internet. This vertical "relationship" can be explained by referring solely to the connection between the individual and the body or business he deals with.

The method of research applied is mainly comparative with the necessary adherence to the dictum of the Supreme Court of Appeal in *Standard Bank Investment Corporation Ltd v Competition Commission and Others; Liberty Life Association of Africa Ltd v Competition Commission and Others*[17] as well as similar views by other South African courts.[18] In the case mentioned Schutz, AJ stated that reference to foreign law is sometimes helpful, particularly when one's own system is silent or uncertain on a point, or for purposes of comparison. He added that there is also sometimes a positive danger in resorting to foreign law, because the person going to it does not sufficiently understand the foreign system.

The reason for using a comparative method of research is that the field of this study has developed very recently and continues to develop rapidly. The different perspectives held in, amongst other jurisdictions, the United States of America and the European Union provide ample substance for a study of this kind.

---

[16] See chapter 2 (2.1.1.2) and page 120 in the list of key terms.
[17] 2000 2 SA 797 (SCA):F-I
[18] See *Blower v Van Noorden* 1909 TS 890:905; *Video Parktown North (Pty) Ltd v Paramount Pictures Corporation; Video Parktown North (Pty) Ltd v Shelburne Associates and Others; Video Parktown North (Pty) Ltd v Century Associates and Others* 1986 2 SA 623 T:640D-E

1.2 Limitation of study

The following limitations are mentioned purely because the inclusion of these issues will lengthen this dissertation unnecessarily and in most instances it can be a study on its own.

(i) The history and development of privacy principles are not investigated because of the limited applicability to this dissertation.

(ii) Not every infringement of the right to privacy over the Internet is dealt with. A distinction can be made between the collection of data by private bodies (for commercial and other purposes)[19] and collection of data by the state (e.g. for the prevention of terrorism).[20] The latter will be mentioned only as illustration or as explanation.

(iii) Jurisdiction is not discussed separately, since it is another issue altogether and will unnecessarily lengthen the dissertation.

(iv) Trade mark protection and intellectual property rights are considered to fall beyond the scope of this study and are only mentioned in passing.

(v) The legitimacy of online contracts and the legal issues pertaining to the development and validity of digital signatures are not investigated, since it represents another field of study and it is not applicable on the topic dealt with in this dissertation.

All the web sites mentioned and referred to in this dissertation were accessed during the course of study in 2003 and they existed at the end of October 2003.

[19] These databases can include credit records, medical records, subscription and membership lists, bank records, telephone records, airline travel records and personal profiles of online service subscribers.

[20] These databases include tax records, bankruptcy records, arrests, marriage licenses, records of property ownership, motor vehicle records, firearm licenses, voter registration lists and school records.

1.3 Information obtainable over the Internet

It is generally known among Internet users[21] that particular kinds of information of a person are necessary to fulfil specific functions as a "person" in cyberspace. In order to fully enjoy the benefits of the Internet, one needs to divulge some information. This information includes, but is not limited to, a name, address, e-mail address, identity number and credit card particulars (especially when making purchases).

In analysing the legal issues in protecting the right to information privacy, it is assumed that the person is connected to the Internet. To connect to the Internet means, without dwelling too much on technical terminology, that a user needs an agreement with an access provider.[22] Access providers provide a variety of services, ranging from an inexpensive dial-up account suitable for a home user to a permanent leased-line connection aimed at commercial use. A user furthermore needs a means of communication with the access provider, such as a telephone line and a modem.[23] Buys[24] simplifies the concept and explains this connection as follows: "The Internet is a collection of packet-switched computer networks, glued together by a set of software protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). These protocols allow networks and the computers connected to them to communicate and share information. TCP/IP creates what is called a *packet-switched network*, a kind of network intended to minimise the chance of losing any data sent over networks. First, TCP breaks down every piece of data into small chunks called *packets*, each wrapped in an electronic envelope with Web addresses for both the sender and the recipient. IP protocol then figures out how the packets are supposed to get from the sender to the recipient passing through a series of routers, like regular mail passes through several post offices on its way to a remote location… [A]s the packets arrive, TCP takes over again, identifying each packet and checking to see if it is intact. Once all the packets have arrived, TCP reassembles them into the original data."

When a person is thus connected the potential exists to collect the following information, whether comprehensively or in part:

---

[21] When the word "user" is appears in this dissertation, it implies a person using the Internet.
[22] An access provider is sometimes also referred to as a service provider. See page 120 for a list of key terms.
[23] Buys 2000:13

1. The IP address[25] of a computer that is connected to the Internet, and information about the Internet provider[26] and services rendered to the user.
2. The user's e-mail[27] address.
3. Information about installed software and computer configuration.
4. Information obtained through the use of cookies,[28] indicating the user's access to web sites,[29] and their activities on those sites, including all sorts of information on logins[30] and passwords[31] required for access to resources and services.
5. Personal data entered by the user while visiting various Internet sites and resources.
6. Personal information that the provider maintains in order to render telecommunications services, including passwords and logins for access to the provider's information systems.[32]

Typically information that can be gathered is not linked to an individual, but rather to a personal computer (PC)[33] or a numerical identifier of such a computer. It is not impossible, though, to link the particulars to a specific person. When personal data becomes known, it is very easy to locate a person as well as unlawfully use these details. For example, if a person's credit card number is known, it is easy for an experienced perpetrator to access other data bases to obtain more information connecting a person to the credit card number.

It is virtually impossible to conceal one's identity and details on the Internet and one almost always leaves a trail in the intangible space that can be traced.[34] This is not always a terrible thing, but one is vulnerable, since details are usually entrusted to a

---

[24] 2000:12
[25] IP is the abbreviation for Internet Protocol. See page 120 in the list of key terms.
[26] An Internet provider is the service provider through which one gains access to the Internet. See page 120 in the list of key terms.
[27] See page 120 in the list of key terms.
[28] See page 120 in the list of key terms.
[29] See page 120 in the list of key terms.
[30] See page 120 in the list of key terms.
[31] See page 120 in the list of key terms.
[32] Naumov 2003
[33] See page 120 in the list of key terms.
[34] To see how vulnerable one really is over the Internet, see Watson 2001:54.

faceless, unfamiliar other “person”. This underlines the fact that the Internet basically relies on relationships of absolute trust and information is the currency of trust.

1.3.1 Consequences of misuse of information

Despite the benefits of information sharing, concerns about privacy are real and legitimate. Many consumers[35] are troubled by the extent to which their information is collected and used. Notwithstanding the fact that one does not have control over one’s own information, significant consequences can result when personal information is misused.

These consequences may include risks to physical security, economic injury that includes patrimonial damage, and unwanted intrusions in our daily lives.

1.3.1.1 Risks to physical security

The fact that information is accessible over the Internet that includes the physical address of a person is reason for concern. Parents do not want information on the whereabouts of their children to be freely available and women may not want their address known for fear of stalkers.

1.3.1.2 Risk of economic injury

The fear of identity theft[36] plagues the information age. Identity theft can range from unauthorised use of your credit card to someone creating a “duplicate you” complete with your birthday and identity number, leaving you with a pile of unpaid bills. This kind of theft tarnishes your credit record, and results in the loss of credit, employment and can even lead to criminal charges for a crime you did not commit.

[35] The word "consumer" is used in its widest sense to mean anybody who uses the Internet and makes online purchases or makes use of services offered over the Internet. A person who simply surfs (see page 120 in the list of key terms) the Internet is referred to as a user.

[36] See chapter 2 (2.1.1.3) on identity theft and page 120 in the list of key terms.

1.3.1.3 Unwanted intrusions

Unwanted phone calls disrupt your quiet time at home and computers are littered with spam[37] sent by a great number of online marketers. There are unwanted solicitations for pornography and other products many find objectionable. Individually, the injury is relatively small, but in the aggregate the harm can be great.

1.4 What is considered to be 'commercial information'?

Commercial information can be regarded as the information necessary to participate in e-commerce[38] and other services the Internet offers. This taken into consideration, personal information can in many instances be regarded as commercial information. Because commercial information contains a component of personal information one can conclude that that other personality related issues will become relevant.

To lay claim to the protection of privacy one must determine whether a personality right exists.[39] Neethling[40] states clearly that privacy embraces all personal facts "wat op die belanghebbende in sy afgesonderdheid betrekking het."[41] Per definition this excludes information pertaining to patrimony.

To determine whether commercial information can possibly be protected as a personality right, an aspect of commercial information, namely creditworthiness, is taken as an analogy. If it is proven that creditworthiness is part of a person's personality rights, this right can possibly be extended to include personal commercial information.

Klopper[42] investigated whether creditworthiness can be regarded as a personality right. He states that creditworthiness is not inherently part of a person and it is not present

---

[37] See chapter 2 (2.2.2) for a brief discussion of spam and page 120 in the list of key terms.
[38] E-commerce is the abbreviated form for "electronic commerce". When the "e-" is subsequently used in front of a word it will have the same meaning. See also page 120 in the list of key terms.
[39] McQuoid-Mason 1978:126. A personality right is defined as part of subjective rights which all human beings possess. Subjective rights are distinguished in five categories according to the legal objects they refer to. Personality rights refer to the objects that concern the human personality, such as a good name, physical integrity, honour, privacy and identity. (Neethling 2002:55)
[40] 1998:38
[41] Privacy embraces all personal facts pertaining to the person concerned in isolation. (My translation)
[42] 1986

since birth.[43] The study deals with the connotation between the *fama* of a person and creditworthiness. Klopper states that "[f]ama in die Suid-Afrikaanse reg word nie spesifiek van kredietwaardigheid onderskei nie en kredietwaardigheid en fama word eerder met mekaar geassimileer as wat daar enigsins 'n onderskeid getref word. Aangesien fama en kredietwaardigheid as sinonieme gebruik word, volg dit dat kredietwaardigheid as synde a faset van die fama deur die lasteraksie beskerm word."[44] Following this statement Klopper tests the attributes of creditworthiness against the attributes of personality rights. He comes to the conclusion that creditworthiness is not a personality right. Klopper further states that: "[creditworthiness] bestaan daarin dat dit 'n vertroueskepping in 'n persoon se *wil* en *vermoë* is om sy finansiële verpligtinge na te kom. Die *wil* om te betaal word van 'n persoon se handelsreputasie, dit wil sê sy gebruik van krediet in die onlangse verlede, afgelei. Hierdie reputasie is nie dieselfde as die fama nie omdat dit verwerf moet word en nie by geboorte ontstaan nie. Dit kan ook verloor word en kom daarbenewens ook 'n regspersoon toe."[45]

It is submitted that the only conclusion to be drawn from the work by Klopper is that creditworthiness, as an aspect of commercial information is an independent immaterial thing and not part of a person's personality rights. As it has been said earlier, for personal information to be protected under privacy principles, it must be proven that such information is protected under a personality right. Since, according to Klopper, creditworthiness cannot be extended to form part of a person's personality, it may be accepted that commercial information *per se* cannot be protected under common law privacy principles. However, these sentiments by Klopper have been discussed recently by Neethling.[46] Neethling states that legal objects such as earning capacity and creditworthiness are called personal immaterial property because they contain elements or characteristics of both aspects of personality and immaterial property. In *Hawker v Life Offices Association of South Africa*[47] it is stated that earning capacity contains both

---

[43] 1986:16

[44] Klopper 1986:192. Fama in South African law is not specifically distinguished from creditworthiness and creditworthiness and fama are rather assimilated than distinguished from each other. Since fama and creditworthiness are used as synonyms it follows that creditworthiness, as a facet of the fama, is protected by the action for defamation. (My translation)

[45] Klopper 1986:249. Creditworthiness exists therein that it is a creation of trust in a person's *will* and *ability* to meet his financial responsibilities. The *will* to pay is deduced from a person's trade reputation, i.e. his use of credit in the recent past. This reputation is not the same as the fama since it must be acquired and does not exist at birth. It can also be lost and is attributable to a legal person. (My translation)

[46] 2001:52 footnote 70

[47] 1987 3 SA 777 (C)

"factors of personality" and "a monetary component". Neethling reveals clearly that earning capacity and creditworthiness display similarities to personality objects, but unlike personality objects, they do not exist separately and independently from the personality. He adds that the relevant legal objects are not purely immaterial property, because they cannot exist independently from their creator. They can only exist during the lifetime of a person and are therefore linked to his personality. Neethling concludes that it is clear that earning capacity and creditworthiness also have a patrimonial nature and a market value and infringement may lead to patrimonial loss.[48]

In the light of the conclusions drawn by Neethling, it can be accepted that the probability exists that immaterial legal objects that cannot exist separately from the personality of a person, may be regarded as intellectual property. However, personal information must be proven to fall in the ambit of this description to be identified as intellectual property to receive the protection granted to intellectual property.

It is submitted that for purposes of this study it serves no purpose to enter into the debate of identifying legal objects. It is accepted that commercial information cannot be regarded as being a pure aspect of the personality.

However, the items a person purchases and the electronic transactions a person enters into, can reflect certain aspects of his or her personality, such as his or her identity. This statement can be explained by referring to the information that is obtainable when a person is active on the Internet. Information gained through various means can reflect a person's preferences and his or her social disposition. This information is used to create profiles and from these profiles inferences can be drawn. Therefore, personality rights can become relevant in some instances.

Another possible alternative may be to argue that, as stated above, commercial information obtainable over the Internet can have a personal character. The object is not to associate aspects of personality, which can be protected under privacy laws, with commercial information (that is not *per se* protected under privacy principles). It is true, however, that the Internet obscures the line of definition. The acquisition of commercial information over the Internet can easily lead to the infringement of privacy, since it is

[48] 2001:53

possible to link a person's identity to his or her commercial information. If commercial information is linked to its proprietor, then his or identity is known and this may lead to infringement of privacy when the holder of such information has malicious intentions. Possible examples of infringement include stalking and the interception of communications.

2. Conclusion

In this chapter, the background of this study was stated and the consequences of the misuse of information have been pointed out for purposes of clarity. However, the list mentioned is not limited to the examples that were provided.

The difficulty of identifying personal commercial information as a legal object was approached with care and the conclusion must be drawn that commercial information cannot purely form part of a person's personality and can therefore not be protected under privacy principles. It has been submitted that the Internet obscures the line of definition and scope should be provided for protecting certain aspects of commercial information that refers to the personality.

The protection of commercial information by applying criminal law principles can also play a role in discovering mechanisms for the protection of commercial data.

Therefore, both possible mechanisms for the protection of commercial data and the protection of personal information, namely criminal law provisions (especially those concerning cybercrime) and protection of (information) privacy, may be relevant and will be discussed without debating the issue of privacy. In the first part of this study the former will receive attention and in the second part the latter will be investigated.[49]

[49] It should be mentioned that the discussion in chapter two can include aspects that overlap with the second part.

CHAPTER TWO
UNAUTHORISED ACCESS TO COMMERCIAL INFORMATION, INCLUDING INTERNET CRIME

1. Introduction

In this chapter the unauthorised access to personal data is investigated.

The issue of access touches two levels. The first involves the question of how to prevent information from falling into the hands of a person with unacceptable intentions. The second level concerns the protection of information from the knowledge of third parties.

Under the first level, computer crime and especially information crime is considered as well as the problems that prosecutors face pertaining to the definition of "property".

The second level of access contentious topics such as data mining, spam and hacking[50] receives attention.

2. Unauthorised Access to personal data

The implication attached to the disclosure of information is that it becomes accessible to another person. The desire to gain unauthorised access to computer systems can be prompted by a number of motives, from simple curiosity to computer espionage.

Access is often accomplished from a remote location along a telecommunications network. Perpetrators can take advantage of lax security measures to gain access or by finding loopholes in existing security measures. They can impersonate legitimate users and gain access to networks by bypassing passwords.

[50] For definitions of these terminologies see page 120 for a list of definitions.

2.1 First level access: Protect information from misuse

2.1.1 Computer crime[51]

This aspect deals with the first level of unsolicited access mentioned above: to prevent information from falling into the hands of a person with unacceptable intentions.

Since the main perspective adopted in this study originates from issues concerning the Internet, Internet crime (or cybercrime) as a component of computer crime will receive more attention. It is true, however that not all research documents make this distinction and the words “computer crime” in many instances also depict situations applying to Internet crime.

The history of computer crime dates back to the 1960s when the first articles on cases of so-called "computer crime" or "computer-related crime"[52] were published in the public press and in scientific literature. These cases primarily included computer manipulation, computer sabotage, computer espionage and the illegal use of computer systems.[53]

To define the concept of computer crime proves to be a mammoth task. The United Nations Manual on the prevention and control of computer-related crime[54] states that a global definition of computer crime has not been achieved but that functional definitions are often proposed. These functional definitions usually only serve a purpose in the context of the study in which they appear.

In the South African Green Paper on e-commerce[55] “cybercrime” is described as "illegal acts, the commission of which involves the use of an electronic system, networks, technologies and devices such as the telephone, microwave and satellite."[56] [57]

---

[51] Computer crime is also referred to as information technology crime (IT-crime), but since the former is embedded in public perception, it will be used subsequently.
[52] Sieber (1998:19) uses both terms synonymously here.
[53] Sieber 1998:19
[54] 1994 par. 21
[55] Available at www.polity.org.za/govdocs/green_papers/greenpaper/
[56] Page 72
[57] See Van der Merwe 2003:33 for a detailed discussion on the relevant definitions proposed by different bodies and authors that does not need further elaboration here.

It is functional to make a distinction between “computer crimes” and “computer related crimes”. The latter requires computers to be used as tools or targets of the criminal offence, but knowledge of the workings of a computer is not essential for the successful commission of the offence. Computer crime can thus be regarded as a criminal offence for which the knowledge of computers is a prerequisite for the successful commission of the crime.

Van der Merwe suggests[58] that the working definition submitted by the OECD[59] in 1986 is adequate for purposes of discussing the subject “computers and criminal law”. This definition reads that “computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data”. This definition is also preferred by Professor Sieber in his study on computer crime commissioned by the European Commission in 1998.[60]

A comprehensive definition for computer crime is provided by the Council of Europe in its report on computer crime:[61]

> “The input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, that influences the result of data processing thereby causing economic loss or possessory loss of property of another person, or with the intent of procuring an unlawful economic gain for himself or for another person.”[62]

Based on this definition a division of five categories of computer crime can be made:[63]

- unauthorised access;
- unauthorised use;
- dishonest manipulation;
- computer sabotage, and
- theft of information[64]

---

[58] LAWSA Vol. 5 par. 11
[59] The United Nations division “Organisation for Economic Cooperation and Development”.
[60] Sieber 1998:20
[61] Recommendation No R (89) 9 adopted by the Council of Ministers on 13 September 1989. (Available at http://cm.coe.int/ta/rec/1989/89r9.htm)
[62] At 245
[63] Van der Merwe 2000:166; 2003:34
[64] See discussion under chapter 2 (2.1.1.2.1)

This definition is functional and wide enough to incorporate hacking and virus-planting.[65]

Sieber[66] distinguishes between four main parts of computer crime with subdivisions:

(i) Infringements of privacy
(ii) Economic offences
    a. Computer hacking
    b. Computer espionage
    c. Software Piracy and other Forms of Product Piracy
    d. Computer Sabotage and Computer Extortion
    e. Computer fraud
(iii) Illegal and Harmful Contents
(iv) Other Offences
    a. Attacks on Life
    b. Organised Crime
    c. Electronic Warfare

This distinction is very helpful in a discussion on computer crime in the broad concept. For purposes of this study only a few categories will be relevant.

Computer crime can be regarded to incorporate a two-fold approach. The first category deals with criminal activity that can only be committed by using a computer system. These crimes did not exist before. They came with the development of technology and a computer is necessary to commit these crimes.[67] In most first world countries these crimes are exclusively created by statute.[68] The second category is much wider and involves crimes that have existed for centuries, but are now committed using a computer system.[69]

---

[65] Virus-planting and Trojan horses are not discussed within the context of this study, but for interest sake it is noted that the Electronic Communications and Transactions Act 25 of 2002 prohibits it in section 86(2). See page 120 for a list of key terms.

[66] 1998:39

[67] These crimes include hacking, cracking and sniffing. (See page 120 for a list of key terms.)

[68] For example in the USA: the Electronic Communications Privacy Act 18 USCS §2510 (1988); the Computer Fraud and Abuse Act 18 USCS §1030 (1991). In Great Britain: the Computer Misuse Act of 1990.

[69] Buys 2000:423. Obvious examples include theft of computer systems, fraud and the possession and distribution of child pornography.

Just as the character of information is altered by the use of computers, the legal paradigm must also change with the new technology to incorporate both above-mentioned categories. As with all changes in technology and society, the law has struggled to keep up with advances in the way people do business. Computer crimes have analogues in South African common law crimes like trespass, larceny, damage to property, but these common law concepts are inadequate to proscribe the new, high technology crimes. These crimes also exist in other countries but they do not cover the technological crimes that are created with the advancement of technology, except in certain instances where special reference is made in statutory instruments.[70] In addressing the problem of computer crime, laws must be expansive enough to deter unlawful activities, while narrow enough to recognise the many legitimate uses of computers and computer networks.[71]

Dealing with computer crime is an integral part of e-commerce. It is necessary for purposes of trust that computer crimes should be defined clearly and that successful prosecution takes place.[72]

2.1.1.1 Legislation concerning computer crime

2.1.1.1.1 Brief background

Despite the multitude of new computer-specific legal questions, the emergence of computer-related criminal law (or criminal information law) can be systematised and traced back to six main waves of computer crime legislations, which today still characterise the six main fields of criminal information law. These six areas are: the protection of privacy; economic criminal law; protection of intellectual property; illegal and harmful contents; criminal procedure law; security law.[73]

The protection of privacy as the first wave of law reform in most western legal systems emerged in the field of privacy protection in the 1970s and 1980s. This legislation was a

[70] See discussion under chapter 2 (2.1.1.2.1.1 and 2.1.1.2.1.2 respectively) on the positions in the United States and the United Kingdom.
[71] Rasch 1996
[72] Van der Merwe 1999:237
[73] Sieber 1998:26

reaction to new challenges of privacy caused by expanded possibilities for collecting, storing and transmitting data by new technologies. "Data protection laws" were enacted and have been constantly revised and updated, protecting the citizens' right of privacy with administrative, civil and penal regulations.[74]

2.1.1.1.1.1 OECD[75]

The OECD has also played a significant role in the development of policy concerning computer crime. The first comprehensive effort dealing with the criminal law problems of computer crime was initiated by the OECD. In 1983 the OECD undertook a study of the possibility of an international application and harmonisation of criminal laws to address the problem of computer crime and abuse.[76] As a result of the committee's proposals, the OECD recommended the member countries to ensure that their penal legislation also applied to certain categories of computer crime. The proposals included a list of acts which could constitute a common denominator between the different approaches taken by the member countries.[77]

In 1986, it published Computer-Related Crime: Analysis of Legal Policy, a report that surveyed the existing laws and proposals for reform in a number of member states and recommended a minimum list of abuses that countries should consider prohibiting and penalising by criminal laws.[78]

In 1992, the OECD developed a set of guidelines for the security of information systems, which is intended to provide a foundation on which states and the private sector may construct a framework for the security of information systems.[79]

The work that the OECD has done in policy development and recommendations through research is invaluable. Although these recommendations do not have official enforceability, they provide a useful basis for member states as well as other countries when compiling national legislation.

---

[74] Sieber 1998:26
[75] The United Nations division “Organisation for Economic Cooperation and Development”.
[76] Sieber 1998:33
[77] See the OECD web site: www.oecd.org.
[78] See the OECD web site: www.oecd.org.
[79] See the OECD web site: www.oecd.org.

2.1.1.1.1.2 Council of Europe

Another expert committee was appointed by the Council of Europe and the legal issues were further discussed leading to the Recommendation No. R(89) 9.[80] This Recommendation was adopted by the Council of Europe on September 13, 1989. This document "recommends the Governments of Member States to take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime… and in particular the guidelines for the national legislatures". It contains a minimum list of offences necessary for a uniform criminal policy on legislation concerning computer-related crime and an optional list, which describes crimes that have already been penalized in some States, but on which an international consensus for criminalization could not be reached.[81]

The minimum list of offences for which uniform criminal policy on legislation concerning computer-related crime had been achieved enumerates the following offences:

- Computer fraud.
- Computer forgery.
- Damage to computer data or computer programs.
- Computer sabotage.
- Unauthorised access.
- Unauthorised interception.
- Unauthorised reproduction of a protected computer program.
- Unauthorised reproduction of a topography.[82]

The subject was also discussed at the 13th Congress of the International Academy of Comparative Law in Montreal in 1990, at the UN`s 8th Criminal Congress in Havana the same year, and at a Conference in Wurzburg, Germany, in 1992.

The Council of Europe adopted another Recommendation concerning problems of procedural law connected with Information Technology on September 11, 1995.[83]

---

[80] This Recommendation is available at http://cm.coe.int/ta/rec/1989/89r9.htm.
[81] See Recommendation No. R(89)9.
[82] Recommendation No. R(89)9.
[83] Council of Europe: Recommendation No. R(95)13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995.

A Committee of Experts on Crime in Cyberspace (PC-CY) was appointed in 1997 in the Council of Europe in order to identify and define new crimes, jurisdictional rights and criminal liabilities due to communication on the Internet. Canada, Japan, South Africa and the United States were invited to meet with experts at the Committee meetings and participated in the negotiations. The Convention was finally adopted by the Ministers of Foreign Affairs on November 8, 2001.[84] It was open for signatures at a meeting in Budapest, Hungary, on November 23, 2001. Ministers or their representatives from 26 member countries together with Canada, Japan, South Africa and the United States signed the treaty. The total number of signatures is 33. Other countries outside the Council of Europe may later be invited to accede to the Convention.[85]

2.1.1.1.2 Current position

The Council of Europe Convention on Cybercrime set out directions for countries to enact national legislation on cybercrime based on the abovementioned treaty.

Penal provision is of vital importance in protecting and preventing information technology from criminal activity. The perpetration itself might appear to be innocent, but illegal access to data or information can cause severe problems. Whenever there is a suspicion of illegal access from system hackers, all data including programs has to be verified for irregularities and viruses.

As a result of the recommendations from the OECD,[86] the Recommendation and the Council of Europe Convention,[87] many countries have made the unauthorised access to data or information liable to punishment.[88]

South Africa is one of the many countries which adopted legislation concerning cybercrime. The Electronic Communications and Transactions Act[89] deals with cybercrime in chapter XIII. This chapter solves the issue of legality and prevents the

[84] This Convention is available at http://conventions.coe.int/treaty/EN/projets/FinalCybercrime.htm
[85] Schjolberg 1999
[86] The United Nations division “Organisation for Economic Cooperation and Development”.
[87] See chapter 6 (4)
[88] See Schjolberg 1999 for a thorough elucidation on the different countries' adopted legislative measures.
[89] Act 25 of 2002. The Act came into force on 30 August 2002 (Proc R68 GG 23809 of 30 August 2002). See further discussion under chapter 5 (3.2)

need to extend some of the definitions of present common law crimes to include computer crimes.[90]

2.1.1.2 Information crime

Without attempting to discuss the broad concept of computer crime any further, it is mentioned that authors have identified five examples of computer abuse, namely financial crime, information crime, theft of property, theft of services and vandalism.[91]

From this list, information crime needs to receive attention. One of the characteristics of information is its intangibility. When not part of a corporeal document, like a paper file, information stays incorporeal. This fact proves to be a major headache especially in an information society where so much relies on the transfer of correct data.

At the same time the criminal law is battling to protect information in a compatible manner. According to the South African common law definition of theft[92] only moveable tangibles that are owned or possessed by another can be stolen.[93]

Another problem originates when it must be proven that the property (information in this instance) was taken away from the owner with the intent to permanently deprive him of ownership. In the instance of theft of computerized information, the "stolen" property remains precisely where it was, and the owner is not deprived of the actual use of the information. Similarly, concepts of trespass and housebreaking do not fit well into the electronic environment.

The South African Trespass Act[94] constitutes the statutory offence of trespass. In section 1 the Act prohibits the entry of or presence upon *land* and the entry of or

---

[90] See discussion under chapter 2 (2.1.1.2.1.3)

[91] Van der Merwe 2000:167

[92] Snyman defines theft: "A person commits theft if he unlawfully and intentionally appropriates movable, corporeal property which (a) belongs to, and is in the possession of, another; (b) belongs to another but is in the perpetrator's own possession; or (c) belongs to the perpetrator but is in another's possession and such other person has a right to possess it which legally prevails against the perpetrator's own right of possession provided that the intention to appropriate the property includes an intention permanently to deprive the person entitled to the possession of the property, of such property.." (2002:469). Burchell and Milton define theft as follows: "Theft consists in an unlawful *contrectatio* with intent to steal of a thing capable of being stolen." (1997:540)

[93] This statement does not include the position pertaining to intellectual property where one deals with

presence in *buildings* in certain circumstances.[95] There can be no uncertainty that this crime cannot, with its current description, be extended to the electronic environment.

Housebreaking with the intent to commit a crime can also not be applied to crimes committed with computers. The definition for this crime[96] in South African criminal law states clearly that this crime entails the entrance into a building or structure (premises) with the intent to commit a crime inside.[97] The fact that entrance must be gained to a building or structure through breaking in, makes it impossible to apply this definition to computer crime.

The most instances of theft or fraud committed successfully with computers reveal that the object of the offence is not the computerised information itself. The information is merely a means to obtain property or some other advantage, which in most cases prove to be money. This occurrence of theft or fraud falls under the definition of "computer related" crimes, since a computer was the means to commit the crime.[98]

2.1.1.2.1 Defining 'property' in relation to computer crime and especially theft of information

Internationally early computer crime prosecutors found problems in employing traditional common law concepts to the new electronic media. Consider the following scenario: former employee of XYZ company, a defense contractor, now works for FGH company, a competitor. His former employer has never deleted his computer account, and he accesses that computer to obtain valuable competitive bid information which he uses to the advantage of his new employer. Has the employee "stolen" the information?

It is clear that the former employer's bid information is sensitive. It is not as clear that such sensitive information is protected by the law. Moreover, it is not even clear that what the former employee did constituted a criminal offense. Clearly it remained in the

---

licences.

[94] Act 6 of 1959

[95] My emphasis

[96] The definition proposed by Burchell and Milton state: "Housebreaking with intent to commit a crime consists in unlawfully breaking and entering premises with intent to commit that crime." (1997:601). See also Snyman 2002:539.

[97] See *S v Lawrence* 1954 2 SA 408 K 409; *S v Meyeza* 1962 3 SA 386 N; *S v Ndhlovu* 1963 1 SA 926 T 927; *S v Ngobeza* 1992 1 SASV 610 T 613H.

former employer's computer, and remained available for the former employer's use. Is the bid information “property” subject to theft at all? If so, what types of information are “property?” Must the information be “confidential” to be “property?” If the former employee accessed the computer and viewed the internal phone directory (which might be publicly available) would prosecution based on theft be warranted? Must the employee know of the confidential -- and hence protected -- character of the information in order to be guilty of a criminal offense?

With the advancement of technology and the fact that assets are being dematerialised in great dimensions, the law of property is struggling to keep track of all the intricacies this dematerialisation entails. The concept of regarding information as property, has posed innumerable obstacles.

In his study on computer crime, Sieber[99] researched the development and mechanisms of privacy protection in different countries. He mentions the following on the development of legislation:

> "Contrary to the legal rules on corporeal objects, information law must not only consider the economic interests of the proprietor or holder of information, but must also take into account the interests of those persons who are concerned by the content of information. Before the invention of computers, the legal protection of those persons was connected with criminal provisions on libel and traditional secrecy protection (e.g., in the medical field). However, these traditional provisions for the protection of personal honour and private secrets only covered part of the personality right and proved to be far too narrow for a protection against the new possibilities of collecting, storing, accessing, comparing, selecting, linking and transmitting data by new technologies. These new threats to privacy prompted many countries to enact, since the 1970s, new bodies of administrative, civil and penal regulations not only in general “horizontal” privacy laws but also in specialised “sectorial” legislation."[100]

---

[98] See definition under chapter 2 (2.1.1)
[99] Sieber 1998:62
[100] Sieber 1998:62

The issue about the nature of information and whether it can be regarded as property is considered by referring to the points of view of the United States, the United Kingdom and South Africa.

2.1.1.2.1.1 United States

The federal system in the United States complicates the making of a general inference concerning the legal position.

In the United States the application of federal common law concepts of fraud, theft and trespass was an ill fit to the new technology. For example, the federal embezzlement statute[101] proscribes the "conversion" of federal property. But is "information" contained on a computer truly "property" subject to conversion? Is all information property, or only certain types of information? Must the defendant be aware that the information is protected in order to be criminally prosecuted? If so, how do you demonstrate such knowledge? Is information subject to greater protection in a computer than it would be in other? Who "owns" corporate or governmental information? Can information be "converted" when the information remains in the possession of the owner? Is the offensive conduct the "theft" of the information, or the later use of that information? What constitutes "use" of information?

Considering information itself as property subject to theft or conversion, while consistent with the axiom that "knowledge is power," represents a potentially dangerous precedent. The federal criminal law protects certain discrete types of information from disclosure or misuse, including national security information, grand jury information, bank secrecy and credit reporting information, probation and pre-sentence reports, personnel and health records, tax records, and records protected from disclosure under the Privacy Act. Federal law also protects certain patent, trademark and copyright information, not from disclosure, but from infringing use. Under state law, various other types of information may be protected - sometimes with potential criminal sanctions, sometimes with evidentiary sanctions, sometimes with purely civil or injunctive sanctions. These include criminal arrest reports, bank records, cable TV records, credit information, criminal justice information, employment records, insurance records (including health insurance),

[101] 18 U.S.C. § 641

mailing lists, medical and treatment information, school records, social security numbers, tax records, and certain telephone records. Finally, in several jurisdictions, state law also protects the disclosure or use of trade secrets.[102]

Rasch[103] is of the opinion that from an American perspective no consensus exists on what types of information can and should be considered property on the network, and what constitutes theft or interference with this property.

The most attractive alternative may be to interpret "property" so widely that information becomes susceptible to theft. This is a controversial point which was followed in *Carpenter v US*.[104] The judge held that the *Wall Street Journal* had a "property right" in keeping secret and exclusive contents of stock market columns. For this reason the *Carpenter* case has often been interpreted as holding that information *per se* is property. This judgement does not seem to be a portrayal of the general feeling concerning this issue.

It seems that American courts are still reluctant to regard information as moveable property for purposes of statutory protection when there is no indication that the information falls under intellectual property.

2.1.1.2.1.2 Britain

The crime of theft was initially broadly defined in the Theft Act of 1968.[105] Section 1 provides that "property" includes "money and all other property, real or personal, including things in action and other intangible property". This definition seemed to address the type of commercial interest in credit and information that needed some kind of protection in dealing with the Internet. However, this section provides that the property should be taken with the intention to deprive the proprietor permanently, something which is clearly not done when information is simply copied.

---

[102] Rasch 1996. See the remainder of this article for a discussion on the protection of information that falls under intellectual property in cases of theft and fraud.
[103] 1996
[104] 108 S Ct 316 (1987)
[105] The Theft (Amendment) Act of 1996 (c.62) broadened the definition to also include "obtaining a money transfer by deception". (A copy of this act can be downloaded from http://194.128.65.3/acts/acts1996/1996062.htm)

Tapper[106] suggests that a possible solution could lie in section 6(1) which provides that:

> "A Person appropriating property belonging to another without meaning the other permanently to lose the thing itself is nevertheless regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the other's rights."

2.1.1.2.1.3 South Africa

In South African law commercial information is as a rule not regarded as personal information since it does not form part of the personality of a person.

In general the requirements for theft include that the perpetrator must appropriate a moveable corporeal thing in an unlawful manner and he must have the intention to permanently deprive the owner of the property.[107] Therefore, three requirements of theft will turn out to be a challenge to prove. Firstly, the requirement that the thing must be corporeal or tangible, secondly, that the thing was appropriated and thirdly, that the perpetrator intended to permanently deprive the owner of the thing.

Snyman adds that the opinion that only corporeal objects can be stolen, should be taken with a pinch of salt. It is clear that the requirement of corporeality is not strictly enforced.[108]

To incorporate business transactions that are conducted virtually and to keep criminal law relevant in the theft of money under these circumstances, the requirement of tangibility of property has been dispensed with. Van der Merwe states that “[t]he definition of “goods capable of being stolen” has been judicially interpreted to also include intangible, abstract sums of money or credit.[109]

---

[106] In Van der Merwe 2000:182
[107] Burchell and Milton 1997:542
[108] 2002:492
[109] Snyman 2002:492; Burchell and Milton 1997:554. See *S v Kotze* 1965 1 SA 118 at 123H; *S v Graham* 1975 3 SA 569 at 575G-H.

Theft can include theft of credit. Therefore, it does not make sense to cling to a relentless requirement that property must be tangible and corporeal. Snyman[110] suggests that this "property" should rather be described as "economic assets", "an abstract sum of money" or "credit".[111]

Burchell and Milton[112] mention significantly that the theft of credit can include the occurrence where a person instructs a computer to transfer money from one account to another.

In *S v Harper*[113] the court decided that shares, in contrast to share certificates, can be stolen. The courts have however, steadfastly refused to extend this principle to the dematerialisation of other types of goods."[114]

In Canada the Court of Appeals decided that information does not constitute property under section 283(1) of the Criminal Code. The case of *R v Stewart*[115] dealt with the theft of confidential information *per se*. It was held that that if protection is warranted for confidential information, it should be granted through legislative enactment and not through the extension of the concept of property or of the scope of the theft provision under the Code.[116]

The Discussion Paper[117] on Computer related crime mentioned that "there is no indication that an extension of the common law offences is likely. This possibility is dependant on the level of appreciation of the dangers of the relevant activities among the judiciary. It is further dependant upon the willingness of the investigating and prosecuting authorities to prepare a case for prosecution in the hope of convincing a court that a common law offence should be extended to apply to a set of circumstances to which it did not apply hitherto."[118] The discussion paper proposed legislation in the

---

[110] 2002:492
[111] Theft of money in the form of credit did not exist in our common law. It was created by the courts.
[112] 1997:556
[113] 1981 2 SA 368 D
[114] Van der Merwe 2003:32; Lawack-Davids 2000:49; In *S v Mintoor* (1996 1 SACR 514 C) the court refused to accept that electric units can be stolen in South African law and the accused was not convicted.
[115] 1988 1 S.C.R. 963 (Available at www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol1/texte/1988scr1_0963.txt)
[116] 1988 1 S.C.R. 963 par. 33
[117] Project 108, discussion paper 99 (published 02-07-2001)
[118] Par. 2.4.2

form of a Computer Misuse Bill[119] to deal with these problems.[120] The proposed bill forms the basis of chapter XIII of the Electronic Communications and Transactions Act (ECT) .[121]

2.1.1.2.2 South African measures against information crime

The ECT resolved the issue whether the common law should be extended to include theft of information as an offence by statutorily prohibiting certain actions. Section 86(1) forbids the unauthorised intentional access[122] to, interception of or interference with data.[123]

It follows that in the example where a person accesses the Internet and obtains certain information about another, the one who had accessed information without authorisation, will be committing an offence. But is there another sanction placed on the unauthorised *use* of such information?

The ECT makes special reference to computer-related extortion, fraud and forgery in section 87.[124] In this section definite crimes are prohibited. From the context the crime of theft is not included, neither is any mention made of the "theft" of information. One can, however, propose that the action of *accessing* information is substituting the notion of applying the principles of theft.

It is submitted that a person who obtains information over the Internet without authorisation or the consent of the "owner" of such information, can only be prosecuted in terms of section 86(1) which forbids unauthorised access. Such a wrongdoer does not interfere with the said data, nor does he deny the "owner" access to the data. If it

---

[119] Annexure A of the discussion paper submits the proposed Computer Misuse Bill.
[120] Par. 2.4.3
[121] Act 25 of 2002 which came into operation on 30-08-2002
[122] Section 85 of the same act defines "access" to include "the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data".
[123] This prohibition applies subject to the Interception and Monitoring Prohibition Act 127 of 1992.
[124] Section 87 reads as follows: "(1) A person who performs or threatens to perform any of the acts described in section 86 [unauthorised access, interception or interference], for purposes of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence. (2) A person who performs any of te acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence."

can be proven that the wrongdoer used “any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data” he can be found guilty of an offence in terms of section 86(3)[125] and (4).[126]

Besides the offences created by the ECT the application of prevalent criminal law principles in the case of common law crimes such as theft and fraud will still be relevant. If a person accessed information unlawfully and he or she uses that information to commit a crime, the crime itself will still be punishable. For example, if a person had access to the information of another without authorisation or consent and obtained a credit card number, the use of the credit card number to make purchases will punishable as fraud or, in the alternative, theft.

In the same way an action for defamation can originate when the *fama* of a person was injured.

A few examples of computer crime that threatens information stored on computers or divulged over the Internet will subsequently be discussed.

2.1.1.3 Identity theft[127]

An aspect of information crime (as part of computer or cybercrime) is identity theft. In this study it is discussed as a separate, independent crime.

Identity theft involves any instance where a person uses someone else’s identification documents or other identifiers in order to impersonate that person for whatever reason.

---

[125] Section 86(3): A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code of any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

[126] Section 86(4): A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data of access thereto, is guilty of an offence.

[127] The concept of "theft" does not carry its normal juridical meaning when referred to the descriptive phrase "identity theft". A more fitting description would be "identity fraud" since it covers a wider area of activity. For purposes of clarity, "identity theft" will be used to include fraud as well as other criminal activities.

An example of identity theft that has increased rapidly in the last few years came to the fore recently when a few of ABSA's clients' accounts were emptied by a perpetrator who gained access to the victim's profiles on the bank's web site pretending to be the victim. The perpetrator loaded software called keystroke logging software which automatically copied everything the victims typed on their computers and sent it back to the fraudster without their knowledge.[128] The software therefore transmitted information about the bank accounts typed in by the clients to the fraudster. The perpetrator has recently been charged on a number of counts of theft and fraud.

An article by Adam Cohen[129] explains this phenomenon plainly: "This software plants itself in the depths of your hard drive and, from that convenient vantage point, starts digging up information. Often it's watching what you do on the Internet. Sometimes it's keeping track of whether you click on ads in software, even when you're not hooked up to the Internet. In Netspeak these programs are known as E.T. applications because after they have lodged in your computer and learned what they want to know, they do what Steven Spielberg's extraterrestrial did: phone home."[130]

In the United States the Federal Bureau of Investigation ascertained that identity theft affects 900 000 new victims each year.[131]

A person's identity might be "stolen" in order to commit financial fraud[132] or other criminal activities.[133] Credit card fraud is the simplest form of identity theft. A potential wrongdoer does not need to go to great lengths to obtain a person's credit card number and the Internet provides ample opportunity for a "thief" to gather an unsuspecting shopper's particulars.

---

[128] Press release by ABSA on 20 July 2003. www.absa.co.za

[129] 2000:37

[130] The same article by Cohen explains "Trojan horses" and gives examples of both as well as the origin of these applications.

[131] Obringer 2002

[132] Financial fraud can include, but is not limited to, bank fraud, credit card fraud, computer and telecommunications fraud.

[133] Criminal activities may be computer and cyber crimes, organised crime, drug trafficking, alien smuggling and money laundering.

The National Consumers League in America made statistics available that illustrates Internet fraud during 2002.[134] Credit card payments form thirty four percent of payment methods overall which provide ground for criminal activity.

A survey,[135] which was reported on in the San Francisco Chronicle, has shown that about seven million Americans were victims of identity theft during 2002. The FTC, which has kept identity-theft reports for the past three years, logged 161 819 complaints in 2002. That was twice as many complaints as in 2001.

The sharp increase in identity theft cases compelled the United States Congress to enact the Identity Theft and Assumption Deterrence Act.[136] This act makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Under this act a name, social security, credit card number, cellular telephone electronic serial number or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual, is considered as "means of identification". In most instances a conviction for identity theft carries a maximum penalty of fifteen years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit the crime.[137]

No statistics on similar cases could be obtained in South Africa. This, however, does not say that identity theft is not a reality in South Africa. In South Africa a person cannot be charged with identity theft and be convicted. In practice a perpetrator will be charged with theft or fraud because of property he stole after obtaining the information. These common law offences most probably will not be extended to include this type of unacceptable behaviour, since no real need exists for such an application. It will

[134] www.fraud.org/2002intstats.htm
[135] Anonymous 2003
[136] This act was enacted in October 1998 and codified in part at 18 U.S.C. §1028.
[137] The FTC made a booklet available online which explains in simple terms what is identity theft and what can be done to prevent it. This booklet is available at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

become clear later in this dissertation that other regulations and legislative provisions meet this requirement.[138]

With the development of technology and widespread access to it, a downside does exist and identity theft is part thereof.

2.1.1.3.1 Practical control mechanisms

2.1.1.3.1.1 Methods and Systems of Payment

Different methods of payment and precautions will be discussed that can possibly protect the identity of the buyer. This list is not a *numerus clausus* and does not pretend to convey all the technical detail concerning the functioning of these systems.

In South Africa legislation has not yet been enacted that regulates payment methods or that stipulates which payment method is preferred or is the safest. The reason may well be since technology is developing and a need for alternative methods of payment have not featured strongly up to now. The Electronic Communications and Transactions Act refers to method of payment under consumer protection. Section 43(5) states:

> "The supplier must utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned." [139]

Section 43(5) covers the spectrum of payment methods that exist and will be developed as long as it is "sufficiently secure with reference to accepted technological standards". The choice of words implies a wide concept pertaining to "accepted technological standards". One must, however, accept that the area that this section aims to regulate is a dynamic field that develops rapidly. The wording of the section can thus be interpreted with reference to current technological standards and will thus not soon become outdated.

---

[138] See discussion about the Electronic Communications and Transactions Act (25 of 2002) under chapter 5 (3.2)

[139] The obligations created in section 43 only refers to suppliers offering goods for sale, for hire or for

2.1.1.3.1.1.1 Payment cards

Payment over the Internet can be accomplished by submitting the details of a payment card to the merchant who then forwards the information to the issuer of the particular card to receive payment for goods or services he rendered.

Three broad categories of payment cards can be distinguished for purposes of online payment, namely credit, debit and charge cards.[140]

Payment by credit card entails the buyer instructing its bank via a payment order to transfer funds to the seller's bank for the credit of the seller. The debit on the account of the seller is paid in accordance with the terms of the contract with the issuer of the card.[141]

When payment is made by debit card, the seller instructs its bank via a payment order to collect funds for it by debiting the buyer's bank. The legal relationships to a debit card are much the same as to a credit card, the principal difference is that the debit cardholder must keep an account that is linked to the card in credit.[142]

Payment by means of a charge card means that the outstanding balance of purchases must be paid after the statement date, either in full or in accordance with the terms of the contract. The function of this card is to facilitate payment and no revolving credit is generally granted.[143]

Payment by means of payment cards poses a great risk, especially when unprotected messages containing payment information is sent. These messages can be intercepted and used to defraud the owner of the card or the merchant.[144]

Central registries for online credit payment present a possible solution. The system operator issues an identification number to each registered user which is connected to

---

exchange by way of an electronic transaction.

[140] Buys 2000:285

[141] Buys 2000:285

[142] Buys 2000:286

[143] Buys 2000:286

[144] See Buys 2000:289 for an evaluation of the card payment system.

the user's card information. When payment is made no sensitive information is sent over the Internet and the need for protection is reduced.[145]

A drawback of this system is that the procedures for verification and confirmation of payment messages by the third party need a lot of time in order to complete the transfer.[146]

A protocol was developed for conducting secure online transactions which will address the issues mentioned above. This protocol, Secure Electronic Transactions (SET) is a joint initiative by the large card-issuing companies to develop a system whereby the integrity of payment messages can be verified through the use of digital signatures.[147]

2.1.1.3.1.1.2 Digital Cash or Electronic Money

This form of electronic payment is relatively new and it has been invented to improve the speed and security of electronic commerce.

Electronic cash is an attempt to construct an electronic payment system modelled after our paper cash system. Paper cash has such features as being portable, recognisable, readily acceptable, transferable, untraceable, anonymous and has the ability to make "change".[148] The designers of electronic money attempted to preserve the features of untraceability and anonymity.

Swart[149] simplifies this concept by stating that "[e]lectronic money in its most basic form consists of a string of numbers identifying it as money in much the same way as banknotes each have a unique identifying number, thereby constituting a token that resembles value". Lawack-Davids[150] is of the opinion that a proper definition can only be found when one distinguishes between the types of electronic money.[151] This she does with such meticulous care and circumspection that a summary would not give due

[145] An example of such a registry is *First Virtual*. (www.fv.com)
[146] Buys 2000:288
[147] Buys 2000:288
[148] Law 1996
[149] In Buys 2000:294
[150] 2000:206
[151] Swart (in Buys 2000:297) also offers criteria to distinguish between the different systems.

credit to her effort. However, her final definition corresponds with the definition proposed by Swart.

For purposes of this study, it will suffice to say that electronic money is a generic term that covers a host of systems which can function in many different ways.

To illustrate this subject further it is necessary to refer to the EFTPOS (electronic funds transfer at point-of-sale) system of payment. EFTPOS allows retail payments to be effected by the transfer of funds electronically from the accounts of customers to the accounts of retailers. The account of the customer is debited and the account of the retailer credited simultaneously.[152] This is the principle on which debit/credit card purchases rely.

EFTPOS-based electronic money systems initiate transfers on conventional bank or credit card accounts, similar to EFTPOS-based systems.[153] An example of this payment method is CyberCash.[154]

CyberCash applies available hardware and software to handle payments. CyberCash functions as an escrow account[155] within the existing banking system. When value is transferred, information regarding the transfer is sent to the bank and the account balances are adjusted accordingly.[156]

Another example of electronic money was invented by David Chaum, who developed the blind signature that allows numbers to serve as money.[157] This technology is utilised in the electronic money system which is called Ecash and operated by DigiCash.[158] Ecash involves the creation of “electronic coins” in the form of digitally signed numbers in exchange for money from the user's bank account. Ecash is designed for secure payments from any personal computer to any other work station, over the Internet (or any other network) or with e-mail. A point of criticism against this system is that the numbers of the coins (or notes) can be copied with relative ease.

---

[152] Lawack-Davids 2000:49
[153] Buys 2000:299
[154] See the CyberCash web site www.cybercash.com
[155] See discussion under chapter 2 (2.1.1.3.1.1.5)
[156] www.cybercash.com
[157] Baase 1997;96
[158] Buys 2000:300 (DigiCash was bought by VeriSign and it is administered by the company)

A large number of systems exist that each operates in a similar manner.[159] Some are hardware based, other rely on software and some need both to function. Electronic money is still in the early years of its development, but the use of electronic money holds a number of advantages over conventional methods of payment. One of these is the reduced operating costs that will save banks and financial institutions huge amounts of money. For the time being, it seems that the popular method of payment, namely payment with payment cards, will continue its dominance in online payments.

2.1.1.3.1.1.3 E-wallets

An e-wallet is a small software program used for online purchase transactions. Many payment solution companies offer free Wallet software that allows several methods of payment to be defined within the wallet (for example, several different credit cards). This is how it works:

- When you order something, the order is sent to the merchant. The merchant (actually, the merchant's server) sends back an invoice and asks the consumer to launch the Wallet in his computer (or to download it quickly if the consumer doesn't have it yet).
- When the consumer selects "Pay," the software on the merchant server sends a message back to the consumer's PC that activates the "Wallet" software. The consumer selects one of the cards defined in the Wallet and clicks.
- The transaction includes immediate credit card authorisation.

ABSA provides a service like this for their clients which they call Secure Online Shopping. The online wallet can be downloaded to a person's computer and be linked to any ABSA credit or debit card. The client's actual card details never travel over the Internet. The bank generates a new number for each online transaction the client makes and it is this number that is sent to the online shopping site.[160]

[159] Swart (in Buys 2000:301) discusses more examples of electronic money, e.g. Visa Cash, OpenMarket and Mondex. (Mondex, a subsidiary of National Westminster, a British bank, operates on the smart card system.)

[160] www.absa.co.za

This payment method is one of the most accessible and safest means to make online payments. The fact that this service is normally offered without charge makes it desirable to the average Internet user. When a financial institution such as a bank offers this service it may prove to be even more popular. The reason is that people would rather trust a reputable institution that has proven its reliability in the past.

2.1.1.3.1.1.4 Electronic Data Interchange (EDI)

Electronic data interchange is the computer to computer transmission of business data in a standard format by way of remote data processing, enabling commercial communication and the conclusion of contracts without human intervention.[161] Smaller businesses started to use the Internet as a medium of communication for conducting EDI with success, although it was initially thought that the open network architecture of the Internet was not suitable for EDI applications.

Some problems exist concerning the security of messages, the conclusion of contracts and the protection of data. It is accepted that the provisions in the Electronic Communications and Transactions Act will in some measure resolve the issues, especially concerning the question of binding contracts and signatures.[162]

2.1.1.3.1.1.5 Escrow services (third party payments)

Third party payment involves introducing a company which acts as a third party to collect and approve payment form one client to another.

The basic way in which escrow payments work is:

(i) Both parties agree to terms of the transaction, which includes a description of the merchandise, sale price, number of days for the Buyer's inspection, and any shipping information.

[161] Buys 2000:290
[162] See Buys 2000:292 for an evaluation of EDI.

(ii) The Buyer submits a payment, selecting cheque, money order, wire transfer or credit card online. Escrow.com verifies the payment. The processing time varies by payment method.

(iii) Upon payment verification, the Seller is authorised to ship merchandise and submit tracking information. Escrow.com verifies that the Buyer receives the shipment.

(iv) The Buyer has a set number of days for an inspection and the option to accept or reject the merchandise.

(v) Escrow.com pays the Seller by cheque or wire transfer. The transaction is complete.[163]

This type of payment can also fall under credit card transactions since some companies offer an alternative that does not involve downloading special software, encryption of credit card information or configuring of a Web browser or other software. All a consumer needs is a VISA or MasterCard and an e-mail account. An example of such a service provider is First Virtual.

The way this system works is that a person signs up for a First Virtual account through their web page, which involves giving a credit card account number. In return, they give you a unique account identifier, a PIN, that you can send over the Internet whenever you want to purchase something from a merchant who also uses the First Virtual system. After you have ordered the item, First Virtual sends you an e-mail message requesting an authorisation to process payment on your credit card. With this virtual credit card escrow service, First Virtual claims that they provide good security without the need for complex encryption and software hassles.

However, this method does have its down side since the third party will have access to all details of the consumers' transactions.

2.1.1.3.1.2 Encryption

The most prevalent method for payment online is still the credit card. To secure credit card payments, the confidential details of the payment are encrypted.

[163] www.escrow.com/solutions/escrow/process.asp

Encryption generally includes a coding scheme, or cryptographic algorithm, and a specific sequence of characters called a "key", used by the algorithm.[164] For an encrypted message to be accessible to the recipient he or she must also possess the key to decrypt the message.[165]

Encryption is essential to the integrity of the financial system. In addition to communications applications, encryption can be used on stored material to protect it from unauthorised access, modification, or theft by outsiders.[166]

Without digression into the technical aspects of encryption it is useful to note that sensitive information can be encrypted in storage as well as during transmission to protect against leaks and intruders.

The other side of the coin is also very relevant. If all messages are encrypted what degree of control does law enforcement bodies have? In the United States this debate is very much contentious especially in the light of terror attacks. An FBI software programme called Carnivore exists, which taps into the networks of phone companies and Internet service providers and can sift through vast amounts of information. Understandably this method of "control" instigated fierce resistance from privacy advocates.

In South Africa the Electronic Communications and Transactions Act stipulates mandatory actions for cryptography providers. Section 29 states that the Director-General of the Department of Communications must establish and maintain a register of cryptography providers that include their names, addresses, a description of the type of cryptography service or product that is provided and other particulars that are prescribed to identify and locate the cryptography provider. Section 30 includes an obligation for the cryptography provider to register before he may provide cryptography services or products in the Republic.

---

[164] Baase 1997:88; Lawack-Davids 2001:3
[165] See Baase 1997:95-107 for a detailed exposition of the technical issues regarding encryption.
[166] Davidson 1998:48

The debate circles around the provisions in section 31 where the disclosure of information contained in the register is restricted (subsection 1). The exceptions to the application of subsection 1 are worded in subsection 2. Together with the Promotion of Access to Information Act,[167] some legal practitioners are concerned about the safety and privacy of the individual since circumstances do exist when information can be disclosed.[168] Subsection (2) states that subsection (1) does not apply in respect of information which is disclosed –

(a) to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings;
(b) to government agencies responsible for safety and security in the Republic pursuant to an official request;
(c) to a cyber inspector;[169]
(d) pursuant to section 11[170] or 30[171] of the Promotion of Access to Information Act, (Act 2 of 2000); or
(e) for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

The key seems to be the balancing of rights of individual privacy against the State's legitimate interests and duty to protect the security of citizens.[172]

2.1.1.3.1.3 Anonymising agents

A number of tools have been developed to help Internet users surf the Web anonymously. These anonymising agents focus on ensuring that requests to Web sites cannot be linked to an IP[173] address from which a person can be identified.[174]

---

[167] Act 2 of 2000
[168] Bidoli 2001:36
[169] Chapter XII deals with the appointment and powers of cyber inspectors.
[170] This section deals with the right of access to records of public bodies.
[171] This section deals with access to health or other records.
[172] Because of the limited relevancy of this issue on the subject of this study a comprehensive discussion is not provided. See Lawack-Davids for a useful and detailed discussion on all the aspects of cryptography from a South African point of view.
[173] Internet protocol
[174] These anonymising agents are also called identity-management products. For a few examples of such products see Ryrie 2000:43

Next to anonymising agents, pseudonym agents exist that help users build persistent anonymous relationships, e.g. to take advantage of customised services.

Anonymity and pseudonym agents are useful when a person is surfing the Web and wants to do so without being identified or supplying personal information. However, when users wish to make online purchases and have merchandise delivered to their doorsteps, they need to provide some identifying information.[175]

2.1.1.3.1.4 Other measures

2.1.1.3.1.4.1 Internet browsers

The programme that a person uses to surf the Internet is called a browser. This software has built-in encryption capabilities that scramble the information you send to a server. Using the most recent browser ensures that the data is protected using the latest encryption technology. This technology also uses a Secure Sockets Layer (SSL), which is an Internet security protocol used by Internet browsers and web servers to transmit sensitive information. The server receiving the data uses special “keys” to decode it.

2.1.1.3.1.4.2 Digital certificates

Another method of prevention is to look for digital certificates that authenticate the entity one is dealing with.

Independent services like *VeriSign* will authenticate the identity of the web site you are visiting. Web sites that use this service will have the *VeriSign* logo.

2.1.1.3.1.4.3 Privacy policies

The information entered on a web site should be kept confidential. An increasing number of Web sites have begun to provide privacy policies that provide the sites'

[175] Cranor 1999:29

information practices. These policies should state different aspects. If a person's personal information is collected, it should give an indication what the information is used for and what rights does the person have concerning his or her information.

Look for these policies and read them carefully. While privacy statements are not the only answer to online privacy risks, the effort should be encouraged and commended.[176]

Services like *TRUSTe* review a company's privacy policy and then allow the company to post the *TRUSTe* logo if its privacy policy follows certain industry standards for consumer protection.[177]

In the South African context the Electronic Communications and Transactions Act provides guidelines for privacy protection by data controllers. It should be noted that the privacy provisions spelled out in the Act do not apply unless the site states that they comply with those provisions.[178] The act, therefore, only makes provision for voluntary compliance by data controllers.[179]

2.1.2 Cookies

The issue of cookies is also a controversial topic.[180] Cookies (or "little brothers" as they are sometimes called) are HTTP[181] headers that consist of a text-only string. The string is usually a set of random-looking letters long enough to be unique to every user. The cookie is sent from the server of the web site the person accessed the first time and is saved on the person's hard drive. When the person accesses that site again, a copy of the cookie is sent with the request to that site. In this way the remote server knows who the person is and that he or she visited the site before and it can keep track of items purchased.[182] The function of cookies is to track electronic activity on web sites and the time a person spend on these sites. This information could be linked to the e-mail

[176] See chapter 3(2.3) for a discussion on the possibility of a contractual relationship emanating from a privacy policy.
[177] See discussion under chapter 2 (2.1.1.3.1.4.3)
[178] Wright 2003:26
[179] See discussion under chapter 5 (3.2 and 4)
[180] Sieber (1998:41) agrees that cookies represent a potential risk to personal data within the Internet.
[181] HTTP is an abbreviation for Hyper Text Transfer Protocol. See also list of key terms on page 120.
[182] Buys 2000:385; FTC privacy policy, available at www.ftc.gov/ftc/privacy.htm

address of the person and sold to direct marketers, mortgage brokers or even the government.

Originally cookies were intended to simplify a person's access to the Internet because he does not need to identify himself every time he accesses a certain web site. More recently cookies have been used to keep track of online-shoppers' habits and preferences through the web sites they visit and the amount of time they spend there. This is also due to the commitment of merchants and service providers to provide a better an integrated service to the consumer.

Governments react differently to the issue of cookies. The EU is of the opinion that no personal data should be collected from Internet users without their express consent. According to the EU's Directive on Data Protection[183] the national Data Regulators of EU member countries have extended powers to control what data can be obtained from persons and to halt the export of data to countries deemed to have inadequate protection.[184]

The United States rely on an industry of self-regulation.[185] Buys[186] quotes the episode in March 1999 when the US Energy Department's Computer Incident Advisory Capability issued a statement that the hype about cookies far outweighs the actual hazards of the technology and that cookies do not compromise the privacy or safety of Internet users. In contrast with this statement the Federal Trade Commission concluded after a wide-ranging survey published in June 1998 that "the industry's efforts to encourage voluntary adoption of the most basic fair information practice principle have fallen far short of what is needed to protect consumers."[187]

[183] See discussion under chapter 4 (3)
[184] Buys 2000:386
[185] See discussion under chapter 3 (2.3)
[186] 2000:387
[187] Boukhari 1998:46

2.2 Second level access: Protecting information from third parties

Certain information is held by, for example Internet service providers (ISP's), credit bureaux or even by companies on whose web sites a person may be registered, that should not be revealed to third parties without the explicit consent of the "owner" of the information. A few examples will serve to illuminate this point. Boo.com was launched in 1999 as fashion web site. By May 2000 Boo.com had liquidated most of its assets. Some assets, including its brand, web site and associated intellectual property were sold to another web fashion company, Fashionmall.com, based in New York City. Most significantly, Fashionmall.com acquired data on 350 000 Boo.com customers with no indication of compliance with Boo.com's privacy policies or EU requirements relating to customer data.

Toysmart.com launched its web site in early 1999. In September 1999 Toysmart became a licensee of TRUSTe.[188] In June 2000 Toysmart was forced into involuntary bankruptcy. A *Wall Street Journal* advertisement for Toysmart.com's assets listed among other things: "intangibles, i.e. URL name, databases, *customer lists*,[189] marketing plans, web site content [and] software intellectual property."[190]

2.2.1 Data Mining

Data mining concerns the matter of third parties obtaining information that was not intended for their use.

Many companies use hardware and software to analyse customer data. This process is called data mining. The information obtained is used for database marketing. Businesses try to find new customers as well as keep the old ones. The process of locating new customers involves first analysing huge amounts of data about current customers to form consumer profiles.[191] This information is mainly obtained from online purchases. Once the desired profile is created, information on a larger group of people

[188] See chapter 2 (2.1.1.3.1.4.3) about TRUSTe
[189] My emphasis.
[190] Winn 2000:227

is searched, looking for those who match the profile. Sources of such marketing lists record all the bulletin boards or other information services accessed by a customer. Access to World Wide Web pages is recorded and this information is then sold for marketing purposes.

This is a frightening thought. A legitimate question is how one can exercise control over information about oneself if it is used by another. The defence of the marketers is that information is only used for marketing purposes. However, it is true that personal information is often collected without the knowledge of the consumer and used in ways that may annoy, embarrass, inconvenience or endanger the person. The fact that the person is unaware that information is being collected or how it is used causes that he or she has no opportunity to consent or withhold consent for its use. Even if a person consented to the collecting of his or her information, it often happens that the information is used for another purpose as the one intended for and for which consent was given.

Baase[192] mentions striking examples: "Receiving ads in one's native language may be appreciated by the recipient, but would a customer be pleased if he or she were on a list of people considered likely to buy a product for adults who are incontinent? One company compiled such a list and made it available through a commercial list broker… Would a customer be happy that a store had a record of how many packs of cigarettes, bottles of brandy or contraceptives he or she buys?"

When one considers these scenarios, the consequences seem immense. In many stores the receipt is computer-generated and lists what has been bought. If the purchase is made with a credit card, the consumer's identity is linked with the sale. The same is true of online purchases. Information about the specific item bought is stored and used to create identity profiles. The mere existence of enormous amounts of transactional data stored in databases can be a risk to privacy.

Some measure of comfort may be found in the ECT which states in section 51 that a party controlling personal information may only use that information to compile profiles for statistical purposes. Such a data controller may sell the profiles and statistical data

---

[191] Boukhari 1998:44
[192] 1997:52

as long as it cannot be linked with a specific person by a third party.[193] Section 50(4) determines that the rights and obligations of the data controller and the data subject in respect of the breach of the principles in section 51, are governed by the terms of any agreement between them (in terms of section 50(2)). If no such an agreement exists, there is no sanction for non-compliance with the principles in section 51, since the subscription to these principles is voluntary.[194]

2.2.2 Spam[195]

Spamming refers to the bulk sending of unsolicited e-mail advertisements to huge numbers of Internet users. Spamming burdens the Internet user with unwanted advertising or long downloading times and also damages ISP's as it slows down their services and causes resentment by subscribers who expect the ISP to control the practice.[196]

In South Africa the ECT solves this issue of spam under section 45.[197] Interesting to note is that is that unsolicited commercial communications must give an opportunity to "opt-out".[198] If the sender of such communications persists in sending the information after he has been requested to cease, he is guilty of an offence. Such an offence is punishable in terms of section 89(1) of the same act, which allows for a fine or imprisonment for not more that twelve months.[199]

---

[193] See chapter 5 (3.2.1) for a more detailed discussion on section 51 of the ECT.

[194] See the wording of section 51 and discussion under 7.2.2.1.

[195] The term "spam" was derived from a Monty Python sketch set in a movie studio cafeteria, where the word "spam" takes over each item on the menu until the entire dialogue consists of "spam, spam, spam". Apparently this so closely resembles what happens when mass unsolicited mail takes over mailing lists that the term has been put into common usage (Malkin & Hambridge 1999).

[196] Buys 2000:381

[197] Section 45 determines: "(1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer – (a) with the option to cancel his or her subscription to the mailing list of that person; and (b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer. (2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication. (3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1). (4) Any person who sends unsolicited commercial communications to a person, who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1)."

[198] See section 45(1)(a)

[199] Because of the limited relevance of this subject to this study no further attention is given to spamming. See Buys 2000:382-384 for information on other countries' regulation of spamming.

2.2.3 Hacking/Cracking[200]

The unauthorised access to computers via the Internet is commonly known as “hacking”. This means that the perpetrator logs on to a computer network, and gains entry to it without having the necessary authority to do so.[201] Normally hackers gain entry to computer systems to find out how they work and to see if they are able to break into the network. A hacker does this usually only for personal satisfaction.

Sieber[202] sums hacking up and says that hacking is usually not carried out with malicious intention, but for the pleasure of overcoming security measures. However, Sieber adds that hacking is still a violation of the integrity of computer systems.

Crackers, however, are perpetrators who do not intend to simply gain entry, but they have ulterior motives when accessing a network. They bring computer systems to a halt or they will make copies of sensitive information for use in an unlawful manner.

In the United Kingdom the Computer Misuse Act of 1990 creates hacking offences.[203] This Act was a model for the South African Law Reform Commission's[204] work on the subject of computer crime and it forms the basis of that particular part of the Electronic Communications and Transactions Act. [205]

The Computer Misuse Act in the United Kingdom[206] creates three offences with regard to access to computers. These offences are:

(i) the unauthorised access to computer material;[207]

(ii) the unauthorised access with intent to commit or facilitate commission of further offences;[208] and

(iii) the unauthorised modification of computer material.[209]

---

[200] See the list of key terms on page 120 for definitions of both terms.
[201] Buys 2000:425; Ebersöhn 2001:24
[202] 1998:42
[203] See Van der Merwe 2003:39 for a comprehensive discussion about the content of this Act with reference to hacking.
[204] In this dissertation the Law Commission of South Africa is consistently referred to by its new name, the South African Law Reform Commission, irrespective of when the relevant project or discussion paper was published.
[205] Act 25 of 2002
[206] This act is available at http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
[207] Section 1 of the Computer Misuse Act
[208] Section 2 of the Computer Misuse Act

The provisions in this act are extensive and deals with intent in committing the crimes that are created. The fact that a perpetrator must know at the moment of committing the offence, prohibited under section one, that the access is unauthorised, is echoed in the definition for "access" in the Electronic Communications and Transactions Act.[210]

The Electronic Communications and Transactions Act prohibits the unauthorised access to, interception of or interference with data. Section 86 of the Act constitutes long awaited offences and it is no longer necessary to adapt common law principles to deal with the phenomenon of hacking and cracking.[211]

2.2.4 Packet sniffing

Information is "broken up" and sent over the Internet in the form of smaller parts, called data packets. These packets are sent to the recipient one by one over the Internet, and the recipient's computer arranges the packets in the correct order and combines them again into one message to be read by the recipient.[212]

When these packets travel across the Internet, they can be intercepted, a copy of the original can be made and the original packet can again be sent on its way. This is known as “packet sniffing”. The perpetrator can read the packets to obtain valuable information.

United States federal law prohibits packet sniffing by providing that anyone who intercepts an electronic communication or intercepts and uses the information obtained can be imprisoned or fined.[213]

South African law provides for the prohibition of packet sniffing through the application of the Interception and Monitoring Prohibition Act.[214] Section 2 of the Act states that

---

[209] Section 3 of the Computer Misuse Act.

[210] The Electronic Communications and Transactions Act defines "access" in section 85 to include “the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data”.

[211] See chapter 2 (2.1.1.2.2) for a discussion of the mentioned section and other articles referring to computer crime.

[212] Buys 2000:428

[213] The Electronic Publications and Privacy Act 18 USCS § 2511 (Available at http://caselaw.lp.findlaw.

nobody may intercept a communication without the knowledge or permission of the person who sent the message. The intentional monitoring of communications to gather personal information, is also prohibited.[215]

Section 86 of the ECT can possibly also be applied to this scenario. This section prohibits the unauthorised access to, interception of or interference with data. Subsection 1 states:

> "Subject to the Interception and Monitoring Prohibition Act, a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence."

The punishment of the aforementioned offence is outlined in section 89(1). This section provides for a fine or a period of imprisonment not exceeding 12 months that can be imposed.

3. Conclusion

Computer crime represents the dark side of the development of technology. Many sources have investigated occurrences of computer crime, compiled reports and made recommendations. Many countries have already criminalised computer crime or an aspect thereof. Especially in Europe many countries have enacted specific legislation concerning computer crime. The Unites States with its combination of federal and state laws also have legislation in place aimed at deterring criminals and setting punishments for perpetrators.

A problem still exists, namely that no uniform set of provisions apply globally. The European Union has attempted to bridge this issue by adopting sets of recommendations and directives. The United Nations and other international bodies put

---

com/scripts/ts_search.pl?title=18&sec=2511

[214] Act 127 of 1992

[215] Section 2 of the Interception and Monitoring Prohibition Act (Act 127 of 1992) reads as follows: "(1) No person shall – (a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or (b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning

forward sets of recommendations. These efforts have lead to huge leaps and undeniable progress in the area of unauthorised access to computer systems and personal information. However, to think that it is possible for a uniform, global set of rules, justified by the borderless nature of the Internet, to apply internationally, seems to be wishful thinking.

A kind of information law or more specifically, information criminal law has been and is developing globally. This new aspect of legal systems deals with the nature of information and the protection of it. This protection implies a wider function than the integrity of computer-stored data, which still has an element of tangibility. Some features of criminal law are being adapted to suit the information age and to apply to the digital world and cyberspace. This step was a necessary extension of the law in most countries, since most criminal law principles cannot easily be extended to incorporate offences committed in cyberspace. Other areas of the law, such as the law of things, cannot on its own provide the necessary protection to individuals, without extending the scope of definitions and concepts that have been determined through the years.

At the same time, it should be mentioned that information crime and identity theft offences, that specifically concern data protection, still need a successful method of deterrence.

South Africa has moved a bit closer to realising this by enacting the ECT and creating certain offences. However, as in most instances of crime, no restitution or compensation is applicable. In the second part of this study other means of protecting personal commercial information are considered, but for the purposes of discussing computer crime one would have to wait and see if the offences and punishments created in the act serve as an effective deterrence for prospective perpetrators.

---

any person, body or organisation."

CHAPTER THREE
PERSONAL ELECTRONIC DATA PROTECTION: UNITED STATES

1. Introduction

The similarity between the provisions regarding data protection contained in the Electronic Communications and Transactions Act[216] and regulations emerging internationally is evident. In many jurisdictions (importantly those of our major trading partners), data protection is legislated: be that by way of sectoral legislation as is found in the US or in general data protection legislation which is found primarily in Europe (under the banner of the European Union). It seems that data protection is no longer an area where the private sector is able to regulate itself without some sort of legislative interference. The United States is the only country which persists in its policy of self-regulation. Furthermore, most countries have now recognised that the creation of legislation in this area without some kind of enforcement mechanism doesn't protect the data subject's right to privacy adequately.

The Data Protection Authority in the Netherlands, the "College Bescherming Persoonsgegevens" (CBP), in conjunction with its Spanish equivalent, did an investigation on the manner in which service providers collect and treat information.[217] It seemed that it was not clear to what extent information about consumers were used for marketing purposes. They found that the Spanish service providers give better information to their customers than the Dutch counterparts. The Spanish service providers mostly had a privacy policy and required the consent of the customers to make information known to third parties. This was not the case with the Dutch service providers.

The investigation emphasised the fact that there exists uncertainty over the determination and use of personal data by the providers and that they are often unaware

[216] South Africa Act 25 of 2002
[217] This was published in the annual report of the CBP. (Available at www.cbpweb.nl/structuur/pag_ handel.htm)

of the rules that protect the privacy of their subscribers. It is normally difficult for the subscriber to get insight into the manner in which the service provider treats his or her personal data. When a person applies for subscription more information than what is necessary for access to the Internet, is often required. The service provider often does not make it clear for what purposes this information will be used. It was also found that service providers who supplied free access to the Internet do not use the personal data of subscribers for marketing purposes more than other providers.

In the report of the investigation the CBP suggested a set of guidelines for the lawful and proper processing of personal information when providing access to the Internet. These rules include the requirement for the necessary privacy provisions and the storing and application of personal data.[218]

The occurrence of the above-mentioned phenomenon is not limited to the countries mentioned. During June 1998 the FTC[219] released a report on Internet privacy. The Commission studied more that 1 400 web sites which were targeted at consumers and found that 85% of these sites collect personal data from users. Only 14% tell the users that they are doing it and only 2% of the sites provided a comprehensive privacy policy telling how data will be used. The FTC chairperson, Robert Pitofsky, said that "concerns about personal privacy are repeatedly cited as the most important reason not to get on the Internet"[220]

In January 2001 Consumers International released its findings of a study that was done on data protection.[221] It found that web sites who sell products and render services to customers all over the world do not comply with international data protection standards. In many instances information about the customer is collected without his or her consent and without the consumer knowing for what purpose the information is used for. They often fail to inform the consumers about their rights and how security is maintained.

The study further showed that although the European Union has strict prescriptions on data protection, many EU sites do not comply with these prescriptions. Ironically

[218] This set of guidelines is available at www.cbpweb.nl/documenten/av_17_Klant_in_het_web.htm
[219] The American Federal Trade Commission
[220] ZDNet 4 June 1998.
[221] Consumers International "Privacy@net: An international comparative study of electronic commerce and data protection."

enough, this study found that many American web sites have better privacy policies than their European counterparts.

They found that out of the 750 web sites studied, just over two-thirds (67%) collected some sort of personal data from their users. Almost all of these sites asked for details that made it easy for them to identify or contact that person. Fifty eight percent of sites that collected information had a privacy policy, but only thirty two comma five percent of them alerted the user of the privacy policy at the time of collecting information. It was also found that privacy policies often do not contain important information and the companies often do not abide by their own policies.

Clearly, data protection is a delicate issue all over the world. In the following paragraphs possible solutions are considered as it is implemented by different countries.

2. Common Law protection of personal data

The principles mentioned underneath are those that apply on federal level. Different state laws are not considered independently.

Different principles may be cited for the protection of personal data that have their origin in common law standards. Some of these principles have been developed and codified.

From the perspective of a database owner in the United States, facts in databases are not eligible for protection under copyright law. In certain cases, however, courts have found common law rights associated with the use or publication of commercially valuable facts, typically under the tort doctrine of misappropriation.[222] This offered an alternative to copyright law in protecting data assets against commercial exploitation. However, this outcome has been limited in subsequent judgements because of a potential conflict with pre-emption principles.[223]

An alternative source for the protection of databases is found in the common law trade secret doctrine. This doctrine generally protects valuable, confidential business

[222] See the landmark Supreme Court case of *International News Service v Associated Press* 248 U.S. 215 (1918) where the "hot news" theory was established.

information from misappropriation where the holder takes reasonable measures to maintain its secrecy.

Some of these principles were enacted in the Uniform Trade Secrets Act.[224] This act defines “trade secret” as:

> Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[225]

The trade secret doctrine has been used in a number of cases to protect customer lists and databases from misappropriation.[226] The issue of secrecy causes an obstruction for database companies that disseminate their products widely and proves to be a remedy of limited application.

The possibilities mentioned above for data protection does not directly concern the individual and will not be discussed in more detail the protection of personal data from an individual's point of view needs more attention. Information or personal data *per se* is not protected by the common law. To guarantee protection, personal data has to qualify as a thing that can be legally protected.

The question arose whether personal information can be regarded as property and can therefore be protected from theft. Initially this possibility was tested against the subject of trade secrets, since it was a known concept. The problem was that a completely new type of legal interest had to be protected, namely two categories of immaterial property, the first one being electronic money or credit or an abstract sum of money, the second

---

[223] Winn 2000:241
[224] 14 U.L.A. 433 (1990 & Supp. 2000) (Available at http://caselaw.lp.findlaw.com/scripts/title_search.pl?title=uscodes&keyword=Uniform+Trade+Secrets+Act)
[225] § 1(4) U.L.A. 438
[226] Winn 2000:244

being simply information, whether it be in the shape of trade secrets, know-how, military classified information, or data collected and systematised in a certain way.[227]

Because of the limited scope of copyright and trade secret protection, database owners have turned to contract provisions to protect their interests.[228] A possible contractual relationship pertaining to privacy policies can develop in future but has not found application in United States law yet. Many web sites post privacy policies that govern their practices with regard to personal information they collect. It is unclear whether the act of posting these privacy policies creates a contractual relationship between the individual visiting the site and the party posting the privacy policy. Claiming that a privacy policy creates a contractual relationship between the individual whose information has been collected subject to it and the web site operator may be a good way to strengthen individual privacy rights on the web, but it poses complications pertaining to enforcement and whether all the requirements for legal contracts were met.

When one seeks to protect data under privacy principles, one must look at the principles of tort. Prior to 1890 no American court recognised a right to privacy. In the following years the courts and legislatures began to apply the doctrine forwarded by Warren and Brandeis in their now famous article "the Right to Privacy".[229] Roos[230] discusses the development of the acceptance of this notion and adds, quoting Prosser,[231] that by 1960 the overwhelming majority of American courts declared that the right to privacy existed in one form or another. From these judgements four torts tied together by the common name “right to privacy”, emerged. These four torts are:

(a) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
(b) public disclosure of embarrassing private facts about the plaintiff;
(c) publicity that places the plaintiff in a false light in the public eye;

---

[227] Van der Merwe 2000:174

[228] *ProCD, Inc v Zeidenberg*, 86 F.3d 1447, (7th Cir. 1996) (Available at http://laws.findlaw.com/7th/961139.html) which was followed by *Hill v Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997); *CompuServe, Inc. v Patterson*, 89 F.3d 1257 (6th Cir. 1996); *Hotmail Corp. v Van$ Money Pie, Inc.*, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998). See also the Uniform Computer Information Transactions Act (UCITA) which applies to “computer information transaction” including commercial agreements “to create, modify, transfer, or license computer information of informational rights in computer information" (§ 102(a)(11) (1999) (Available at http://caselaw.lp.findlaw.com/scripts/title_search.pl?title=uscodes&keyword=Uniform+Computer+Information+Transactons+Act)

[229] 1890 Harvard Law Review 193

[230] 1990:267

[231] "Privacy" 1960 California Law Review 383 385-388

(d) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[232]

Roos adds that these four privacy torts are, realistically speaking, not of much practical value for data privacy protection.[233] She maintains that the "intrusion upon seclusion" tort may come closest to the issue of invasion of data privacy, but it cannot deal with all data privacy issues.

Under United States law, privacy rights of individuals in general and information privacy rights in particular are a patchwork of different statutes and common law doctrines that provide a certain amount of protection for individuals in some contexts.[234] Edmund Andrews summarised this position in the New York Times: "U.S. privacy laws are far more lax and consists of a hodgepodge of statutes and regulations enforced by various state and federal agencies charged with oversight of other industries, like, for instance, those that regulate banks."[235]

2. Statutory protection of information privacy

The right to privacy in the United States is not expressly mentioned in the Constitution but has been held to be guaranteed under the umbrella of the First, Third, Fourth, Ninth and Fourteenth Amendments.[236]

Buys[237] mentions that constitutional protection of information privacy in the United States is a thorny issue. It seems that the Fourth Amendment, more that any other constitutional provision, indicates the reality of such a right. The Fourth Amendment states:

"The right of the people to be secure in their person, houses, paper and effects, against unreasonable searches and seizure, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation,

[232] Because of limited application, these four torts will not be discussed.
[233] 1990:268
[234] Winn 2000:250
[235] Andrews 1998
[236] *Griswold v Connecticut* 381 US 186; *Roe v Wade* 410 US 113
[237] 2000:373

and particularly describing the place to be searched, and the person or thing to be seized."

In *Katz v United States*[238] electronic eavesdropping on private communications was held to be an infringement of the Fourth Amendment, since it constituted a search and seizure invading the privacy of the communicator. The realm of the Fourth Amendment pertaining to the protection of information does not stretch very far. In *United States v Miller*[239] the U.S. Supreme Court found that the Fourth Amendment does not protect the expectation of privacy when an individual voluntarily conveys information on cheques and deposit slips to a bank. The depositor takes the risk that the information will be conveyed to the government and these documents cannot be considered confidential communications.

The U.S. Courts have also examined whether the control of personal information by individuals to whom it relates is a fundamental right protected by the Fourteenth Amendment.[240] It was decided by the Supreme Court that individual control of personal information is not protected by the Fourteenth Amendment and that fundamental private privacy rights include only those relating to marriage, procreation, contraception, family relationships, child rearing and education.[241]

Tribe[242] can suitably be quoted in this context:

"In an information-dense technological era, when living inevitably entails leaving not just informational footprints but parts of one's self in myriad directories, files, records and computers, to hold that the Fourteenth Amendment does not reserve to individuals some power to say when and how and by whom that information and those confidences are to be used would be to denigrate the central role that informational autonomy must play in any developed concept of the self."

---

[238] 389 US 347 (1967). Available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=389&page=347

[239] 425 US 435 (1976). For a summary of the facts see Dunlop and Kling 1991:454. This judgment is available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=425&page=435

[240] The Amendment deals with due process.

[241] See *Paul v Davis* 424 US 693 at 712 (1976); *Nixon v Administrator of General Services* 433 US 425 (1970)

[242] In Buys 2000:374

While the courts are still to extend the scope of this amendment to also protect information privacy, there is no single primary law that protects personal data in the scope of the Internet. There are a number of federal and state laws that protect the privacy of certain forms of personal information.

3.1 Fair Credit Reporting Act[243]

The U.S. Congress recognised the concerns of sensitive information that is exchanged by credit reporting agencies and other businesses in 1970 and the Fair Credit Reporting Act (FCRA)[244] was enacted. This was the United States' first major privacy protection law. This act ensures the integrity and accuracy of consumer reports and limits the disclosure of such information to entities that have "permissible purposes" to use the information.[245]

The Act is, however, concerned "primarily with the accuracy of the reporting system and secondarily with preventing the unauthorised disclosure of consumer information".[246] The aspect of privacy is undermined to a certain degree since credit reports may contain information on an individual's "character, general reputation, personal characteristics, or mode of living".[247]

The scope of this act's application is also limited since it only applies to credit information gathered and used by government agencies and credit bureaux.

3.2 Privacy Act

The Privacy Act of 1974[248] regulates the federal government's use of personal data and concerns the vertical relationship between the government (or its agencies) and the individual.[249] This law was passed in part because of concerns in the 1960s and early

[243] See Roos 1990:478 for an in depth overview of the FCRA.
[244] 15 United States Code § 1681 *et seq* (Available at http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=15&sec=1681)
[245] For a discussion on the FCRA see Baase 1997:56; www.epic.org/privacy/fcra/default.html
[246] McQuoid-Mason 1978:44
[247] 15 U.S.C. § 1681d(a) (Available at http://caselaw.lp.findlaw.com/casecode/uscodes/15/chapters/41/subchapters/iii/sections/section_1681d.html)
[248] 5 U.S.C. § 552a
[249] Section (a)(4)-(5)

1970s about many abuses by the federal government (and in particular the Watergate scandal). The abuses included wiretappings, mail openings, burglaries and questionable use of personal records.[250]

The stated purpose of this act is to provide certain safeguards for the individual against an invasion of personal privacy, by requiring federal agencies to:

i) permit the individual to determine what records pertaining to him are collected, used or disseminated by such agencies;
ii) permit the individual to prevent records pertaining to him, obtained by such agencies for a particular purpose, from being used for another purpose without his consent;
iii) permit the individual to gain access to information pertaining to him in federal agency records, to have a copy made of all or any portion thereof and to correct or amend such records;
iv) collect, maintain, use or disseminate any records of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use and that adequate safeguards are provided to prevent misuse of information;
v) permit exemptions from the requirements with respect to records provided in this Act, only in those cases where there is an important public policy need for such an exemption and has been determined by statutory authority;
vi) be subject to civil suit for damages, which occur as a result of wilful or intentional action, which violates any individual's rights under this Act.

The Act prohibits an agency from disclosing a record by any means to any person or agency, unless such disclosure is authorised by the individual to whom the record refers. Exceptions do exist for when non-consensual disclosure is acceptable.[251] If such an agency fails to comply with this prohibition and an individual is adversely affected, the latter can bring a civil action for damages.[252]

[250] Baase 1997:49
[251] 5 U.S.C. § 552a a(b)
[252] 5 U.S.C. § 552a (g)(1)(D)

Although this act was an important step in the protection of privacy from abuse by the federal government, there are problems with it. It has many loopholes and is not being effectively enforced. For example, an individual cannot compel an agency to disclose information. The act only applies where a record is kept about an individual in a system of records by a federal agency.[253] The only remedy is actual damages after the fact, provided it can be proved that the agency acted intentionally[254] and that the action had an adverse effect on him.[255]

3.3 Electronic Communications Privacy Act

In addition to protecting the data contained on computers, federal law also attempts to protect the integrity or confidentiality of electronic communications. The Electronic Communications Privacy Act of 1986 (ECPA)[256] protects all forms of electronic communications from unlawful interception and disclosure, and unlawful access to stored communications. Since the enactment of the ECPA it was scrutinised in various court cases. In *McVeigh v Cohen*[257]a navy officer was discharged after the navy had ascertained that the naval officer was a homosexual by obtaining subscriber information from America Online. This information was gathered without first obtaining the required court order and warrant, in violation of the Act. The court commented that in these days of “big brother”, where through technology the privacy interest of individuals is being ignored or marginalised, it is imperative that laws explicitly protecting these rights be strictly observed.

In May this year, in *In Re Pharmatrak, Inc. Privacy Litigation*[258], the U.S. Court of Appeals for the First Circuit suggested that data collection by a third party might violate provisions of the ECPA. The court held that specific consent was required by the party whose information is gathered.[259]

---

[253] The act provides definitions for the words "record" (§ 552a (a)(4)) and "system of records" (§552a(a)(5)).
[254] 5 U.S.C. § 552a (g)(4)
[255] 5 U.S.C. § 552a (g)(1)(C-D). For a detailed analysis of the Privacy Act see Roos 1990:264.
[256] 18 U.S.C. § 1028 (Supp. IV 1998)
[257] 983F Supp 215 (D) DC 1998
[258] Available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=1st&navby=case&no=022138&exact=1
[259] See discussion by Anita Ramasastry at http://writ.corporate.findlaw.com/ramasastry/20030604.html

3.4 Communications Assistance for Law Enforcement Act

In 1994 the Communications Assistance for Law Enforcement Act (CALEA) was enacted. According to this act telecommunications equipment must be designed so that the government can intercept all wire and electronic communications originating from or coming to a particular subscriber.[260]

3.5 Gramm-Leach-Bliley Act

On November 12, 1999, the Gramm-Leach-Bliley Act (GLBA) became law. Title V of the Act protects the financial privacy of consumers by (i) limiting the instances in which a financial institution may disclose nonpublic personal information about a consumer to nonaffiliated third parties; and (ii) requiring a financial institution to disclose to all of its customers the institution's privacy policies and practices.[261] The GLBA defines non-public personal information as personally identifiable financial information that is provided by a consumer to a financial institution or obtained by such an institution through a transaction or other method.[262]

The GLBA requires financial institutions to provide privacy notices to consumers, and allows consumers, with certain exceptions, to choose whether their financial institutions may share their information with third parties. In February 2000 the Federal Trade Commission (FTC) released draft regulations[263] under the Gramm-Leach-Bliley Act that aim to enforce these directions on financial institutions.[264]

---

[260] A later change in CALEA provided that information services (e.g. bulletin boards and Internet services) are exempt from the requirement that their systems be designed for government interception.

[261] Available at http://caselaw.lp.findlaw.com/scripts_search.pl?title=15&sec=6801

[262] Section 6809 defines non-public personal information in subparagraph 4 as: ""(A) personally identifiable financial information - (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. (B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title. (C) Notwithstanding subparagraph (B), such term - (i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but (ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information."

[263] See also the Financial Privacy Requirements of the GLBA summarised by the FTC available at www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

[264] "Financial institutions" is defined broadly under the proposed regulations and includes businesses

Important to not is that the keyword here is "financial institutions". The GLBA defines "financial institution" as follows:

> "The term "financial institution" means any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12.[265"266]

Each of the above-mentioned acts has a limited range of operation as was indicated in each instance. The total area of protection these acts offer seems to be the sum of privacy protection regarding personal data American statutory law provides.

Different states have also enacted legislation in variety of contexts that create privacy rights or impose conditions on the use of personal information. In November 2000 there were more than 300 on-line privacy bills, aimed at the use of personal data, pending in state legislatures.[267]

In the light of the GLBA the state of California introduced the California Financial Information Privacy Act in December 2002 (but it has not been enacted yet). This bill emphasises the Legislature's intentions for financial institutions to provide their consumers notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions.[268]

The awareness of the protection of personal information on national or federal level in the United States of America seems to have an impact on state level. The different states experience the responsibility to protect their residents from the unauthorised access and collection of personal data.

A body that plays a mentionable role in the attempt to regulate privacy principles and enforces legal provisions on the Internet is the Federal Trade Commission.[269]

---

engaged in the extension of credit.

[265] Available at http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=12&sec=1843.

[266] 15 U.S.C §6809

[267] Winn 2000:254

[268] This bill is available at http://www.leginfo.ca.gov/pub/bill/sen/sb_0001-0050/sb_1_bill_20021202_ introduced.html

[269] More information on the initiatives of the FTC is available at www.ftc.gov/bcp/conline/edcams/

4. Other measures

The events of September 11, 2001 had a devastating impact on the concept of privacy in the United States as established principles came into reconsideration. The main concern was for national security rather than for individual privacy.

No better proof of this attitude can be found than in the acceptance of the USA PATRIOT Act[270]. A Few days after the terror attacks, the U.S. Senate voted to grant the Federal Bureau of Investigation sweeping Internet surveillance powers that in some cases would not require a judge's approval. Huge portions of that bill, titled the Combating Terrorism Act, eventually became part of the even more grandly named law called the USA PATRIOT Act.[271]

It seems, however, that there are signs that Congress realised it went too far in allowing electronic surveillance and other invasions of personal privacy. On 22 July 2003 by a 309 to 118 vote the U.S. House of Representatives approved legislation that would essentially block part of the USA Patriot Act that permitted police to seek a court order that let them surreptitiously enter a home or business.[272]

Strangely enough it is apparent that no online privacy legislation exists in the United States. Many have called for such protective measures as it will also increase consumer confidence in the Internet. Another advantage would be that federal legislation could help to ensure consistent regulation of information collection practices across the fifty states.

Objections that are often voiced are that to legislate broad-based privacy protection is extraordinarily difficult. What hampers progress is that technology develops so rapidly that legislation may prove to be outdated even before it can be implemented. Furthermore, no consensus exists about the implementation of privacy principles.

---

infosecurity/index.html

[270] Officially called the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

[271] For more information on this controversial act, see http://writ.findlaw.com/ramasastry/20030217.html. For a copy of the act: www.epic.org/privacy/terrorism/hr3162.html.

[272] McCullagh 2003

In a rapidly changing and dynamic medium, unnecessary regulation of commercial activities can lead to significant unintended consequences, distorting the development of the electronic marketplace. Internet business models must evolve rapidly to keep pace with the breakneck speed of change in the technology, and laws are likely to be outmoded by the time they are enacted.

The Americans opt for a system of self-regulation where legislation does not govern the policies of e-commerce. The industry itself should set rules and standards that should be uphold. This system also attempts to regulate the protection of personal data but the effort seems to be in vain.

In America it seemed that an alternative to these traditional approaches was needed to effectively establish appropriate industry privacy practices. What was needed was a solution that brings to bear the weight of government oversight, the forces of market dynamics and the pressure of public scrutiny. The alternative they prefer is called *self-governance.*

Self-governance is a three-dimensional system that leverages these pressure points to maintain and enforce appropriate practices. Unlike self-regulation, self-governance requires that industry not act alone; rather, it must work in concert with existing laws and develop best practices. Self-governance relies on an informed marketplace that demands disclosure of privacy practices and the opportunity to exercise choice about how information is used. The government must fulfil its role by enforcing existing laws and assuring that industry continues to work toward ubiquitous adoption of best practices. Media and advocacy groups act as a collective conscience by scrutinising the development of self-governance to assure it remains true to its underlying principles and goals and meets the challenges of evolving technologies and business models.[273]

The Online Privacy Alliance[274] was created in 1998 by about 50 companies and associations in America. Members of the alliance support effective self-regulatory

[273] The TRUSTe White Paper - Building Trust Online: TRUSTe, Privacy and Self Governance. The document can be downloaded from www.truste.org/about/trustewhitepaperfinal.doc
[274] www.privacyalliance.org/

policies and manage a privacy seal programme.[275] The alliance provides guidelines for online privacy policies[276] but the organisation was criticised for failing to deal with enforcement issues.[277]

Perhaps the clearest indication that the self-governance approach is on one level working for the United States is the evolution and success of online privacy seal programs, such as *TRUSTe*.[278] A nonprofit, global initiative operating independent from both industry and government, *TRUSTe* was launched to provide a mechanism by which Web sites could alleviate consumer concerns about privacy online. The core of this initiative was the *TRUSTe* Privacy Seal, a visual symbol that could be displayed by Web sites that met the programme's requirements for data gathering and dissemination practices, and agreed to participate in its dispute resolution process. *TRUSTe*'s goal was to establish a seal that would send a clear signal to consumers that they could expect companies to adhere to certain requirements about the way Web sites handled data, and that an independent, third-party would hear and respond to their complaints and resolve their disputes. The backbone of the *TRUSTe* program is the contract that is signed between *TRUSTe* and the Web site. This contract gives *TRUSTe* the ability to address users' privacy concerns regardless of their citizenship or the location of the *TRUSTe* licensee.

Opinions on the failure of self-regulation exist as well. Simon Davies, of the human-rights group Privacy International, already in 1998 said: "I can't find one example of self-regulation anywhere in the world that works for the benefit of the consumer. Self-regulation is a confidence trick, a sleight of hand… If an organization's prime directive is the exploitation of personal data, self-regulation is a contradiction in terms."[279]

The absence of the enforcement methods and sanctions when an organisation does not adhere to its privacy policy may be the main reason for the diverse opinions on the success of self-regulation.

[275] www.privacyalliance.org/resources/enforcement.shtml
[276] www.privacyalliance.org/resources/ppguidelines.shtml
[277] Craddock 1998
[278] See more at www.truste.com
[279] Glave 1998

In reaction to the point of view of the United States, the European Union has adopted a very strong stance on the privacy of Internet users and does not always deem the American system satisfactory. In practice, it seems that EU sites do no better at keeping their users informed than the American sites. In fact, it appears that many European web sites do not comply with the strict rules set by the EU. This may be since the Americans do not have legal protection in this area and that companies have to go to great lengths to reassure their users of security and that their privacy will be protected.[280]

In January 2001 the Online Privacy Protection Act of 2001 was introduced in the House of Representatives.[281] This bill regulates unfair and deceptive acts and practices in connection with the collection, use and disclosure of personal information. The bill provides for the creation of self-regulatory incentives. A very useful definition for personal information is offered by this bill. The term “personal information” is defined to mean information collected online from an individual that identifies that individual, including first and last name; home and other physical address; e-mail address; social security number; telephone number; any other identifier; or information that is maintained with, or can be searched or retrieved by means of, data described in the preceding list.

In the past year, the United States Department of Homeland Security has announced a new cyber security initiative that will include the establishment of a national cyber security division.[282] What that will entail, has not yet been spelt out clearly.

5. Conclusion

In the United States of America personal data is protected by several statutes and indirectly by the Constitution. However, no single piece of legislation exists that, in its entirety, is comprehensively aimed at the protection of personal data. Consequently no entity can enforce the protection of personal information over the Internet, unless a statute makes provision for certain instances.

---

[280] Consumers International "Privacy@net: An international comparative study of electronic commerce and data protection."
[281] This bill is available at http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.89:
[282] Liikanen 2003

To overcome this obstacle a system of self-regulation was introduced that requires businesses and other commercial entities to comply with certain rules that are determined amongst themselves.

There exist entities that act as watchdogs or overseers to make sure that personal information is protected over the Internet. These entities require that businesses subscribe voluntarily. When these businesses comply with the set standards, the businesses are allowed to display the “overseer” entity’s logo on its web site. This creates trust among the public who regularly visits web sites who display these logos.

The system of self-regulation has been criticised in the past and many other countries do not recommend such as system. The European Union prefers a much stricter approach, as will become evident in the following chapter.

CHAPTER FOUR
PERSONAL ELECTRONIC DATA PROTECTION: EUROPE

1. Introduction

Data protection in Europe and especially in the European Union is a much-debated topic. The European Union realised that the protection granted by national privacy principles is in many instances inadequate to protect information in an electronic society. This resulted in the adoption of a number of Directives compelling member states to review their national policies on data protection.

In this chapter the position in Europe will be considered with reference to the common law position as well as the Directives that have been implemented into national legislative instruments.

2. Common Law protection of personal data

2.1 United Kingdom

The English position differs greatly from the law in the United States. Winfield and Jolowicz[283] mentions that an infringement of privacy (which they discuss as a "doubtful tort") may be described as some form of interference with another's seclusion of himself, his family or his property from the public. The common law does protect this right but does so in an indirect manner. [284] There is no direct decision on the point that recognises any general right of privacy, although extensive protection is given against harsh intrusions on the privacy of a person's property.

[283] 1989:555

[284] In a more recent judgement on this issue, that of *Malone v Metropolitan Police Commissioner* 1979 Ch. 344 where telephone tapping was concerned, counsel for the plaintiff did not contend for a general right of privacy.

3. Statutory protection of information privacy

3.1 European Union

The general Data Protection Directive (General Directive) of the European Parliament and of the Council[285] on the protection of individuals with regard to the processing of personal data and on the free movement of such data was adopted on 24 October 1995 and required implementation not later than three years after this date. Member countries of the EU were required to enact the Directive's provisions before the effective date in local legislation. On 15 December 1997 the specific Directive[286] concerning the processing of personal data and the protection of privacy in the telecommunications sector was adopted by the European Parliament and the Council. The date for this Directive's transposition was aligned with that of the General Directive.

The specific Directive of 1997 had to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services. Therefore, on 12 July 2003 another Directive was adopted.[287]

The Internet makes it possible to access and transfer data to any country in the world; once such data is transferred to a country without adequate protection laws, further control of their use may become impossible.[288] The existing national legislation on data protection as well as the EU General Directive contains important rules and remedies to ensure the free movement of such data and prevent its misuse. Based on the EU Directive, the Member States have an obligation to provide for the enforcement of the data protection principles set forth in Article 6 of the Directive. These principles determine that Member States must provide that personal data must be

---

[285] 95/46/EC. The formal name of the Directive is the "European Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data". The Directive is available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEX numdoc&1g=EN&numdoc=31995L0046&model=guichett

[286] 97/66/EC

[287] Directive 2002/58/EC. (Available at http://europa.eu.int/servlet/portail/RenderServlet?search= DocNumber&lg= en&nb_docs=25&coll=in_force=NO&an_doc=2002&nu_doc=58&type_doc= Legislation) Article 19 of the new Directive repealed the directive of 1997 with effect from 31 October 2003. All references that were made to the repealed Directive must be construed to make reference to the new Directive.

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes;
(c) adequate and relevant;
(d) accurate and up to date;
(e) only kept for the necessary period.[289]

The Directive defines “personal data” to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[290] From this definition commercial information which causes a person to be identifiable, can be considered to be “personal information”.

The data controller[291] or user must respect these principles and allow Internet access to the personal data held by it.

According to Article 22 of the Directive, Member States shall provide the right to a judicial remedy for any breach of personal data principles.[292] If the controller breaches the principles, the injured person is entitled to receive compensation from the controller

---

[288] Fazekas in Wilhelmsson 2001:144

[289] Section 6 of the Directive in its totality reads as follows: "(a) "Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."

[290] Article 2

[291] Article 2 of the Directive also defines a "controller": "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing or persona data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law."

[292] Article 22: "Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question."

for the damages suffered. The compensation is based on the national law applicable to the process in question.[293]

The General Directive seeks to prevent abuse of personal data and lays down comprehensive rules, including an obligation to collect data only for specified, explicit and legitimate purposes, as well as to only hold data if it is relevant, accurate and up to date.[294]

3.1.1 Implementation into national law

3.1.1.1 Austria

The Directive has been implemented by the Data Protection Act 2000. The "Bundesgesetz über den Schutz personenbezogener Daten" entered into force on the first of January 2000.[295]

The Data Protection Act establishes a fundamental right to Data Privacy in section 2 "insofar as he has an interest deserving such protection".

Because of its federal structure and the separation of responsibilities between the federation and the "Länder", the directive can only be implemented at the level of the federation in the sectors which fall under its responsibility. (This is the case for the whole area of automated data processing.)

In 2000 the ordinance on standard processing operations has been adopted implementing the data protection law 2000 (and thereby as well directive 95/46/EC). It entered into force on 1 July 2000.[296] In this ordinance some “routine” data processing operations whose maximum content is precisely fixed by this ordinance are excepted from the notification obligation to the data processing registry held by the data protection

[293] Fazekas in Wilhelmsson 2001:144
[294] Buys 2000:376
[295] Datenschutzgesetz 2000, BGB1. I Nr 165/1999 of 17.08.1999. Available at www.bka.gv.at/ datenschutz/ dsg2000e.pdf
[296] Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 – StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification.

commission. For certain other data applications this ordinance foresees a simplified notification obligation.

3.1.1.2 Belgium

The implementation law has entered into force on 1 September 2001 after a public consultation during 1999.[297]

A specific issue that emerged was the one under the heading of e-commerce. The Data Protection Authority has adopted an opinion recalling the privacy principles applicable in the framework of electronic commerce. The opinion describes the circumstances under which personal data are collected on the Internet, and the obligations of the data controller as regards to the information of the data subject, and the proportionality of data collected. The Data Protection Authority insists in the opinion on the need to obtain the consent (opt in) of the data subject before sending unsolicited e-mail messages, and recalls that sending of e-mail using addresses collected on public spaces of the Internet is illegal. The opinion also recalls the main principles applicable to cross border data flows.

3.1.1.3 Denmark

The Act on Processing of Personal Data[298] (the official translated title) was adopted on 31 May 2000 and entered into force on 1 July 2000. The act implements the general Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[299]

The act substitutes the Public Authorities' Registers Act and the Private Registers Act.

[297] Belgian law of December 8, 1992 on privacy protection in relation to the processing of personal data, as modified by the law of December 11, 1998, implementing Directive 95/46/EC. Available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&1g=EN&numdoc=31995L0046&model=guichett

[298] Act No. 429 of 31 May 2000

[299] See www.datatilsynet.dk/eng/index.html for the English version of the Act.

3.1.1.4 Finland

The Finnish constitution guarantees every citizen's private life and honour and the sanctity of the home. Article 6 states that "[e]very Finnish citizen shall be protected by law as to life, honour, personal liberty and property."

Protection of privacy has been a basic right in Finland since 1 August 1995. Under the Finnish Constitution, protection of personal data is regulated by a separate act.

In 1988 the first Personal Data File Act (the official translated title) came into force, representing the first law concerning data protection in Finland. The Act was to prevent violations of integrity at all stages of data processing. The functional objective was to promote the development of, and compliance with, good data processing practices.

The Directive was enacted with the Personal Data Act,[300] which entered into force on 1 June 1999.[301] This act replaced the Personal Data File Act but the main principles of the protection of privacy remained largely unchanged. One of the objectives of the Act is to improve the opportunity of individuals to control the use of their personal data. Individuals have the right to know why and how personal data is being processed and to decide about the processing, unless otherwise stipulated by the law. The Data Protection Ombudsman and the Office of the Data Protection Ombudsman provide guidance and advice on all issues related to the processing of personal data and control the observance of the law.

The Act was amended on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are, in matters concerning the transfer of personal data to countries outside the Union, were incorporated in it.

3.1.1.5 France

In the spring of 2000, the Government requested the National Commission for Informatics and Freedom (CNIL) as well as the Advisory Committee on Human Rights (Commission consultative des droits de l'homme), for an opinion on a preliminary draft

[300] 523/1999

law concerning the protection of individuals with regard to the processing of personal data and amending Law No 78-17 of 6 January 1978 on data processing, files and freedoms. The draft law was adopted by the Council of Ministers on 18 July 2001. Having been submitted to the National Assembly, this draft had been examined at the beginning of January 2002 and adopted.[302]

3.1.1.6 Germany

In the course of modernising German data protection law, the Federal Government is following a two-phase approach.
The first one was in substance directed towards implementing the Directive. On 14 June 2000 the Federal Government (Bundeskabinett) agreed on a draft law amending the German data protection law.[303] The Chamber of State representatives (Bundesrat) made comments to this draft law on 29 September 2000. On 13 October 2000 the draft law amending the German data protection law and other laws was submitted by the Federal Government to the Bundestag.[304] Discussions in the various committees of the Federal Parliament (Bundestag) started in 2000 and were concluded by the law modifying the Federal Data Protection Act and other Acts as of 23 May 2001.[305]

Subsequent to this novellisation, the second phase is aiming at a fundamental reform of data protection law. An important step in this direction has been made by handing over the expert report on the modernisation of data protection law ("Modernisierung des Datenschutzrechts") on 12 November 2001 to the Federal Ministry of the Interior.

The German Federal Data Protection Act[306] as of 1 January 2002 defines “personal data” as "any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)".[307]

---

[301] www.tietosuoja.fi
[302] www.assemblee-nat.fr/dossiers/cnil.asp
[303] The Federal Data Protection Act or Bundesdatenschutzgesetz (BDSG) (20 December 1990, Federal Law Gazette I 1990 p. 2954 with amendments)
[304] BT-Drs. 14/4329
[305] Federal Law Gazette Vol. I p. 904.
[306] Information about this act us available at www.bfd.bund.de/information/engltext1.html.
[307] "… Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)"

This definition is wide enough to include commercial information. The fact that mention is made to "any information concerning the personal or *material* circumstances"[308] supports this statement as well as the fact that the data identifies an individual. Commercial information can do exactly that.

3.1.1.7 Greece

The data protection law has been implemented by Law 2472/97[309] on the Protection of the individual with regard to the processing of personal data. This law has been adopted on 10 April 1997 and entered into force the same day.[310]

Section 2 of the Act defines “personal data” as:

> "[A]ny information relating to the data subject. Personal data are not considered to be the consolidated data of a statistical nature whence data subjects may no longer be identified."

This definition is also wide enough to incorporate commercial information. The identifiability requirement for personal data confirms this statement.

3.1.1.8 Ireland

A draft bill[311] was presented to Government in July 1998.

Ireland has finally implemented the 1995 Data Protection Directive five years after the expiry of the EU's deadline.

Most of the provisions of the Data Protection (Amendment) Act 2003[312] have come into force on 1 July 2003. The remainder, including provisions relating to registration and enforced subject access, do not yet have a date for coming into force.

---

[308] My emphasis
[309] As amended by Laws 2819/2000 (Official Gazette 84 A 15.03.2000) and 2915/2001(Official Gazette 109 A 19.05.2001)
[310] The English version is available at www.dpa.gr/legal_eng.htm
[311] The draft bill was a general outline of proposed legislation.
[312] Data Protection Act available at www.dataprivacy.ie/6ai.htm

3.1.1.9 Italy

The General Directive was transposed into Italian law by Act no. 675 of 31 December 1996, the Data Protection Act.

This statute provides that all the provisions concerning the protection of individuals and other entities with regard to the processing of personal data and all the related measures had to be included into a consolidated text by the end of 2002, in order to facilitate consultation and operational coordination.

3.1.1.10 Luxembourg

Luxembourg adopted a data protection law in 1979 to protect natural or legal persons against the abusive use of data during processing. This law regulated both the public and private sector and is administered by a Consultative Commission, although enforcement was mainly ministerial.

The draft Luxembourg law transposing the General Directive was presented to the Parliament on 7 December 2000.[313] Only Luxembourg is still to implement the Directive.

3.1.1.11 The Netherlands

The Constitution of the Netherlands did not include a general right to privacy until 1983, although there were particular provisions to protect some privacy rights.

The Dutch Data Protection Act which bears the date of 6 July 2000 implements the General Directive into Dutch law.[314]

The new law replaces the act of 28 December 1988, but there is a great degree of continuity from one to the other act.

[313] www.chd.lu/fr/portail/recherArch/recheravan/list.jsp?resSet=4

[314] An unofficial English translation of this act is available on the web site of the Dutch Data Protection Authority: www.cbpweb.nl

3.1.1.12 Portugal

The Directive was transposed into national law in 1998, by the Data Protection Act.[315]

The Portuguese Data Protection Authority gave Opinions during 2000, regarding matters directly connected to the European Union activity.[316]

3.1.1.13 Sweden

The General Directive was implemented in Sweden by the entry into force of the Persona Data Act[317] on 24 October 1998.[318] This act replaced the out-dated Swedish Data Act of 1973.

Secondary legislation[319] came into force on the same day. The new legislation has been fully applicable since 1 October 2001.

3.1.1.14 Spain

The most significant event was the coming into force of Organic Law No 15/1999 on the protection of personal data on 14 January 2000.

This act, like many of the other European Union member countries, makes provision for a Data Protection Authority and the Spanish equivalent is the Agencia de Protección de Datos.

3.1.1.15 United Kingdom

There had been several attempts to get legislation on the subject of privacy. A Home Office Committee in 1972 came out by a majority against the introduction of any general

---

[315] Law 67/98 of 26 October.
[316] These include the data protection adequacy of Hungarian laws, Swiss laws and the Safe Harbor principles; the joint secretariat for the supervisory bodies of Europol, Schengen and Customs; and the personal data processing by the Institutions and bodies of the Community and the freedom of circulation of those data.
[317] 1998:204
[318] www.datainspektionen.se/in_english/default.asp?content=/in_english/legislation/data.shtml
[319] The Personal Data Ordinance 1998:1191

right of privacy, though proposing alteration or clarification of some existing legal rules. The majority felt that a general right would be too vague and uncertain and that it might interfere with free speech.

In 2000 the Data Protection Act 1998 came into force.[320] The Act requires anyone processing, obtaining or disclosing personal data to comply with the eight data protection principles:

The data must be

(i) fairly and lawfully processed;
(ii) processed for limited purposes;
(iii) adequate, relevant and not excessive;
(iv) accurate;
(v) not kept longer than necessary;
(vi) processed in accordance with the data subject's rights;
(vii) secure; and
(viii) not transferred to countries without adequate protection.[321]

Exemption from the Act is given where compliance could prejudice national security or crime prevention and detection.

The collection of personal data, especially by computer, even without publicity, is sometimes brought under the heading of privacy but the problems of control of collection, of security and of access can clearly only be dealt with by a statutory scheme, such as exists under the Data Protection Act (2000). This contains civil liability for damage caused by inaccurate personal data.

This legislation ensured that the United Kingdom had implemented the provisions of the General Directive. Implementation enhanced the framework of rights and responsibilities that had previously been available under the Data Protection Act of 1984. Secondary legislation was also introduced to give effect to the provisions of the Act.

---

[320] www.hmso.gov.uk/acts/acts1998/19980029.htm
[321] United Kingdom Parliamentary Office of Science and Technology "postnote". Available at www.parliament.uk/post/home.htm

Section 1 of the Act provides a definition for personal data. This definition includes data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of the data controller.

Notably the identifiability requirement is also present in this definition. It can be assumed that commercial information, for example a person's credit card number, is included since an individual can be identified if the data controller has the particular number and he is in possession of information that links the number to a person.

The responsibility for the enforcement of the Act falls to the Information Commissioner, who investigates reports of non-compliance and advice businesses to ensure their practices comply with the law.

In a press statement by the EU on 25 July this year[322], the first day of the new regulatory framework for electronic communications in Europe, it was declared that only five Member States have taken the necessary action to transpose the package into national law. These five countries are Finland, Denmark, Sweden, United Kingdom and Ireland. This package refers to all the directives involved that forms the framework for the protection of data.

3.1.2 Conclusion on the position concerning the EU Member States

At this state the inference may be drawn that the European Union has a very strict approach to the issue of data protection. This has led to the enactment of several acts concerning data privacy by the Member States.

The Directive, and the acceptance thereof, represent the staunch perspective held by the European Union. It is also this perspective that struggles to tolerate the more liberal attitude of the United States relating to data protection.

[322] Available at http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/0301121|0|RAPID&1g=EN&display=

3.1.3 Influence on America

EU officials had generally determined that United States privacy protection would not provide an "adequate level of protection". The European Union's determination that the United States' privacy protections were "inadequate" was significant because it would have hindered certain transfers of personal data to the U.S. However, in July 2000, the United States Department of Commerce negotiated the Safe Harbor agreement[323] to the Directive (the "Safe Harbor" to provide a means for U.S.-based companies to avoid interruption of their business operations with the EU and avoid regulation and prosecution by EU authorities under the Directive). By certifying with the Safe Harbor, EU organisations may be assured that U.S. companies have "adequate" privacy protection, as detailed under the Directive.

Compliance with the Safe Harbor principles grants United States companies the following benefits: (1) the 15 European Member States must abide by the European Commission's finding of adequacy; (2) companies that comply with the Safe Harbor will be considered to provide "adequate" privacy protections and data flows to these companies will continue uninterrupted; (3) the requirement for Member States' prior approval of data transfers will either be automatically granted or waived; and (4) charges brought against American companies by E.U. citizens will be heard in the United States, subject to certain exceptions.[324]

3.1.4 Influence on South Africa

The General Directive of the EU puts into affect the principle that any country within the European Union would be prohibited from exchanging data with a country which do not have adequate legal protection of the privacy of personal information.

It is important to note that SA was “blacklisted” by the European Commission for not having an adequate level of data protection. To ensure that data between South Africa and Europe (South Africa’s main trading partner) can be exchanged freely, the

[323] http://profs.lp.findlaw.com/privacy/6.html
[324] The list of companies that have chosen to comply with the Safe Harbor may be found at the Department of Commerce's Web site, www.export.gov/safeharbor

importance of adequate regulation of privacy of information could not be underestimated.

South Africa was forced to review its position concerning the protection of personal data and the Electronic Communications and Transactions Bill saw the light. Heyink[325] mentioned before the ECT was adopted, but after the Bill was introduced, that one would hope that in dealing with this issue that the urgency of the establishment of a workgroup of the Law Reform Commission to address the current deficiencies is both realised and acted upon with considered haste.

This was done and the ECT was enacted. The provisions in the act should prove to be adequate to guarantee that data can be exchanged freely between South Africa and the European Union.[326]

4. Conclusion

The protection of personal electronic data in Europe and especially the European Union is clearly much more formal than the protection the United States' system of self-regulation provides. Data protection is granted through an independent piece of legislation that specifies how personal information should be handled.

The legislation adopted by the member states roughly corresponds since they are all based on the same original document.

An important fact is also that the legislation adopted by the member states makes provision for punishment if the requirements were not adhered to. This serves as a means of deterrence.

[325] 2002
[326] See 7.2.3 for a comparison between the ECT and the applicable EU Directives.

CHAPTER FIVE
PERSONAL ELECTRONIC DATA PROTECTION: SOUTH AFRICA

1. Introduction

Personal data in South Africa is protected through the right to privacy. The protection of commercial information is not mentioned *per se*, but it is submitted that cases may occur when the principles governing privacy may be applied to protect commercial information.

The Electronic Communications and Transactions Act[327] is a statutory instrument that makes provision for the protection of personal electronic data.

The protection of personal data will be considered with reference to South African common law as well as statutory law.

2. Common Law protection of personal data

South African jurisprudence has experienced little difficulty in recognising the right to privacy as an independent right of personality. This affirms the fact that personal information is protected.

The court in the *locus classicus* on this recognition, *O'Keeffe v Argus Printing and Publishing Co Ltd,*[328] identified the right to privacy as one of the personality rights relating to *dignitas*.

In *S v A*[329] the accused was found guilty of *crimen iniuria* because they installed a wireless bugging device in the apartment of the complainant and listened in on his communications. It was held that an invasion of an individual privacy sets a *prima facie* impairment of his *dignitas*. Acting Judge Botha stated that "[t]here can be no doubt that

[327] Act 25 of 2002
[328] 1954 3 SA 244 (C)

a person's right to privacy is one of those real rights, those rights *in rem* related to personality, which every free man is entitled to enjoy".[330] Botha AJ also stated that "I have no doubt that the right to privacy is included in the concept of *dignitas*…"[331]

As a general principle it is accepted in our law that the unauthorised collection of personal information on an individual, without justification, constitutes a wrongful intrusion of his privacy.[332]

In *Universiteit van Pretoria v Tommie Meyer Films (Edms)Bpk*[333] an invasion of privacy was regarded as an aspect of impairment of *dignitas* under the *actio iniuriarum*.[334] It follows then that for a common law action to succeed the plaintiff must prove the elements of the delict, as discussed below.

The Appellate Division in *National Media Ltd and Another v Jooste*[335] confirmed that the individual concerned is entitled to dictate the ambit of disclosure of facts. Harms JA gave much attention to the "privaathoudingswil" of the respondent. The learned judge stated: "I am of the view that a person is entitled to decide when and under what conditions private facts may be made public. A contrary view will place undue constraints upon the individual's so called "absolute rights of personality".[336] It will also mean that rights of personality are of a lower order than real or personal rights. These can be limited conditionally or unconditionally and irrespective of motive. This does not mean that the delictual nature of the claim is thereby compromised."[337]

The elements of the delict will be considered briefly in order to provide a thorough background to the requirements that should be present to constitute a delict.

---

[329] 1971 2 SA 293 (T)
[330] At 297D. Cf *R v Umfaan* 1908 T.S 62 at p. 66
[331] At 297H
[332] *S v Bailey* 1981 4 SA 187 (W)
[333] 1979 1 SA 441 (A); (1977 4 SA 376 (T))
[334] This does not exclude the possibility of an action for patrimonial loss under the *lex Aquilia*.
[335] 1996 3 SA 262 (SCA)
[336] *Minister of Justice v Hofmeyr* 1993 3 SA 131 (A) quoted by Harms JA

2.1 Elements of the delict[338]

2.1.1 Invasion

As was shown above, the South African courts have regarded invasion of privacy as an impairment of *dignitas* under the *actio iniuriarum*.

Neethling[339] clearly distinguishes between two instances when privacy may be infringed. These two instances are firstly, the unauthorised acquaintance with private facts and secondly their disclosure.

2.1.2 Wrongfulness

The wrongfulness of an infringement of privacy is determined in accordance with the criterion of reasonableness or *boni mores*.[340] According to the positive law wrongfulness could arise from the infringement of a subjective right (personality right) or from the breach of a legal duty.

Apart from intrusion and disclosure, mentioned above, the mere unauthorised recording of private facts is also in principle wrongful.

Justification for wrongfulness includes the traditional grounds of justification such as necessity, self-defence, consent, and statutory or official capacity. The grounds of justification applicable in defamation cases, especially privilege and fair comment, should also justify an infringement of privacy.

2.1.3 Intent

An essential requirement for liability under the *actio iniuriarum* is *animus iniuriandi* or intent. *Animus iniuriandi* is presumed once the wrongfulness of the infringement of

---

[337] At 271I-272B
[338] See discussion by McQuoid-Mason 1978:34; Devenish 1999:145; Neethling in Strauss 1988:116
[339] LAWSA vol. 20 par. 178
[340] See *S v A* 1971 2 SA 293 (T); *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C) at 248; *S v I* 1976 1 SA 781 (RA) at 788-789

privacy has been proved. The intention of a defendant is tested subjectively. The question of the reasonableness of the defendant's conduct concerns lawfulness which is tested objectively.

Although the common law does protect privacy to a degree, there does not exist a common law principle that protects personal information *per se*. Therefore, it is comprehensible that specific legislation was required.[341]

3. Statutory protection of information privacy

It is interesting to note that the South African constitution makes an inherent distinction between the different aspects of the right to privacy. Section 14 determines that everyone has the right to privacy, which includes the right not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed.

This section explicitly uses the word "includes" which does not preclude another aspect of the right to privacy. In this sense one can make a classification of privacy from the Constitution:

i) spatial privacy: this includes the rights as it is set out in section 14 (a), (b) and (c).
ii) relational privacy: this is set out in subparagraph (d).

The last distinction can possibly be read to also include information privacy. This, together with the almost unlimited scope of section 14, determines that there may well be a broad protection of information in the Constitution but no detailed guidelines or parameters.

This right in the Constitution protects information to the extent that it limits the ability of people, organisations and the government to collect, publish disclose or use information about others.[342] The right itself is not absolute.[343] It can be limited by a law of general

[341] Van der Merwe 2000:158
[342] McQuoid-Mason in Chaskalson 1998:18

application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.[344]

Most of our law, statutory and non-statutory, was made with either an idea of commerce which did not include electronic commerce or without even reflecting on the impact of electronic ways of engaging in commercial activity.

The process to determine an electronic commerce policy for South Africa started in September 1998 when research started which led to the drafting of a Discussion Paper.[345]

It was decided that the OECD[346] position[347] would be used as the basis for the course of action. The OECD position provided an outline for debate where issues pertaining specifically to South Africa could be pointed out and be debated widely.[348]

3.1 Green Paper on E-commerce[349]

The Green Paper was compiled by the Department of Communications with the purpose to provide a platform from which to translate topical issues concerning e-commerce into government policy. The document was designed to raise questions on issues that needed to be addressed. Some of the issues put forward were the conclusion of contracts over the Internet, the admissibility of electronic evidence and consumer protection. It was recognised that a new legal framework had to be adopted relating to e-commerce. The protection of privacy and personal information was identified as an aspect that also needed consideration.

---

[343] See *Case v Minister of Safety and Security* 1996 3 SA 617 (CC)
[344] According to section 36 of the Constitution (Act 108 of 1996).
[345] Discussion Paper 99, Project 108
[346] The United Nations division "Organisation for Economic Cooperation and Development".
[347] See discussion in chapter 6 (3)
[348] Buys 2000:108
[349] Available at www.polity.org.za/govdocs/green_papers/greenpaper/

3.2 Electronic Communications and Transactions Act (25 of 2002)

The enactment of the Electronic Communications and Transactions Act (ECT) has been recognised as the most significant legal step that South Africa has taken to log on to the world of electronic communications and e-commerce.[350] This act came into operation on 20 August 2002.

3.2.1 Personal information

The ECT provides a comprehensive definition for "personal information" in section 1. The definition given, is quoted in its entirety for purposes of discussion afterwards:

> "personal information means information about an identifiable individual, including but not limited to –
>
> (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
> (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
> (c) any identifying number, symbol, or other particular assigned to the individual;
> (d) the address, fingerprints or blood type of the individual;
> (e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
> (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
> (g) the views or opinions of another individual about the individual;

[350] Jansen 2002:17; Rens 2003:23

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but excludes information about an individual who has been dead for more than 20 years."[351]

This definition is very encompassing and mentions a number of examples regarded as personal information. Again, these examples do not exclude other possible instances. The section plainly states that the examples are include but that personal information is not limited to them.

Although the list is not limited to the examples a few of them can be read to include commercial information. Subparagraph b mentions information relating to financial transactions in which the individual has been involved. This example can be construed to also include commercial information obtained in electronic transaction. The "identifying number" can include a person's credit card number since records exist that can link the number to the person.

Therefore, it is submitted that commercial information is protected under the ECT as a part of personal information.

Chapter VIII applies to the protection of personal information gathered through electronic transactions.[352]

Section 51 of the ECT deals with the electronically collecting of personal information by a data controller and states nine principles that a data controller can comply with.[353]

[351] The definition of “personal information” supplied by the Promotion of Access to Information Act (2 of 2000) is exactly the same as this definition.
[352] Section 50
[353] See chapter 5 (3.2)

When one considers chapter VIII of the ECT, at first sight, a contradiction seems to appear in section 50(1) and (2). Subsection (1) states that a data controller *may* voluntarily subscribe to the principles in section 51 by recording such fact in any agreement with a data subject, while subsection (2) says that a data controller *must* subscribe to all the principles in section 51 and not to parts thereof.[354] The reasonable interpretation is that if a data controller chooses to subscribe to the principles outlined in section 51, he is compelled to subscribe to all the principles. He cannot single out some principles from the list supplied in section 51.[355]

3.2.2 Internet Service Providers

The ECT also regulates the issues concerning ISP's. Chapter XI[356] deals extensively with the limitation of liability of service providers.

The act defines “service provider” in section 70 to mean any person providing information system services.

A very important aspect is that liability of service providers may only be limited if the service provider is a member of the representative body that section 71 provides for and if the service provider has adopted and implemented the official code of conduct of that representative body.[357]

It is of some value to note that an ISP also falls under the definition of "data controller" and is subjected to the provisions set out in section 51.

[354] My emphasis.
[355] See also discussion under chapter 5 (3.2)
[356] Sections 70-79.
[357] Section 79 sets out the occasions when chapter XI does not affect other situations. This include “(a) any obligation founded on an agreement; (b) the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law; (c) any obligation imposed by law or by a court to remove, block or deny access to any data message; or (d) any right to limitation of liability based on the common law or the Constitution.

4. Comparison between the ECT and the EU Directives[358]

When one attempts to delve into the provisions of the ECT concerning personal data protection and examine the substance thereof, it is sensible to compare it with a standard that is widely accepted. The EU Directives most probably meet this standard, since it represents the basis on which the member states of the European Union established their national legislation.

4.1 Directive 95/46/EC

Directive 95/46/EC (general directive) in its entirety deals with the issue of personal data protection. The ECT contains only one chapter (chapter VIII) that determines the South African position. It is understandable that the Directive will contain much more detail. The challenge is to see whether, or not the ECT can compare with the essential requirements for data protection.

It can be accepted that definitions will differ since the functionality of the descriptions will be determined in the context of a document. However, it is helpful to evaluate differences in definitions.

Directive 95/46/EC defines a "controller" to mean "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".[359] The Directive goes further and also defines "processor" as a "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".[360]

[358] Directives 95/46/EC and 2002/58/EC
[359] Article 2(d)
[360] Article 2(e)

The ECT defines "data controller" as "any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject."[361] The ECT does not distinguish between a processor and a controller and both terms are evidently understood under the definition of "data controller". The definition proposed by these two documents for "personal data" or "personal information" has already been quoted in the body of this dissertation and it can be stated that the definition of the ECT includes more examples than that of the Directive.

The general directive makes provision for the implementation of provisions by Member States that guarantee data quality. This is outlined in article 6 of the directive. Interestingly enough, this document distinguishes between principles relating to data quality[362] and criteria for making data processing legitimate.[363] In the ECT no such complex distinction is made. The ECT mentions a number of principles under the umbrella of “principles for electronically collecting personal information”. The content of chapter VIII of the ECT and the general directive corresponds in many instances.

To compare the content of these two documents, it is functional to start from the point of view adopted in the general directive and in each instance the entire article or section is quoted for intelligibility. The substance of articles 6 and 7 is weighed against the principles included in the ECT.

Article 6 of the general directive states:

> “1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

[361] Possible uncertainty may stem from the word "person" but the act intercepts this by defining "person" to include a public body (Section 1). This comprehensive definition supplied by the ECT is reassuring since it incorporates everyone who has contact with persona data of other people

[362] Article 6

[363] Article 7

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with."

Article 7 determines:

"Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent;[364] or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data re disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

[364] The Directive defines 'the data subject's consent" as any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (article 2(h)).

The abovementioned principles regarding the processing of data is largely based on the basic principles for data processing that the OECD suggested in 1980 in the “Guidelines on the Protection of Privacy and Transborder Flow of Personal Data”.[365]

Section 51 of the ECT includes these principles:

(1) "A data controller must have the express written permission of the data subject[366] for the collection, collation, processing or disclosure of any personal information, unless permitted to do so by law.
(2) A data controller may not electronically request, collect, collate, process or store personal information which is not necessary for the lawful purpose for which the personal information is required.
(3) The data controller must disclose in writing the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without express written consent, unless permitted to do so by law.
(5) The data controller must for as long as the personal information is used and for a period of at least a year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or with the written authorisation of the data subject.
(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
(8) The data controller must delete or destroy all personal information which has become obsolete.
(9) A party controlling personal information may use it to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the

[365] See chapter 6 (3)
[366] Data subject: "any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act."

profiles or statistical data cannot be linked to any specific data subject by a third party."

4.1.1 Consent

The consent of the data subject is dealt with in section 51(1) of the ECT and article 7(a) of the general directive. The Directive sets a condition, namely that personal data may be processed[367] only if the data subject has unambiguously given his consent.[368] In this instance the ECT goes further and requires the express *written* consent of the data subject for the collection, collation, processing or disclosure of any personal information.[369]

The ECT limits the actions that need the consent of the data subject to collection, collation, processing or disclosure. No specific reference is made to the recording or storage of such data in connection with obtaining written consent.

4.1.2 Purpose

The purpose of processing[370] personal data is addressed in article 7(b) to (f) of the general directive and section 51(2) and 51(3) of the ECT. Section 51(2) of the ECT maintains that no personal data may be processed which is not necessary for the lawful purpose for which it is required. The following subsection compels the data controller to disclose the specific purpose for processing in writing. The Directive provides a list in article 7 of examples that qualifies as “lawful purposes”.

The Directive as well as the ECT places a restraint on the processing or use of personal information. The Directive mentions in article 6(1)(b) that personal data must be

---

[367] The Directive uses the word “process” and defines it as follows: “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”

[368] See footnote 364

[369] The rest of the subsection determines that the consent of the data subject is not necessary when an action by data controller is permitted by or required by law.

[370] For the sake of functionality the word “process” will henceforth be used to include or represent the definition put forward by the Directive as well as the specific terms used in the relevant subparagraph of the ECT.

collected for specified, explicit and legitimate purposes and the ECT in section 51(4) states that the personal information may only be used for the disclosed purpose.

Article 6(1)(c) demands that personal data must be adequate, relevant and not excessive in relation to the purpose. This provision attempts to prohibit the acquisition of information that is not necessary for the purpose of processing. A similar provision appears in the ECT. Section 51(2) stipulates that only information that is necessary for the lawful purpose for which the information is required, should be obtained.

4.1.3 Records

The ECT requires of a data controller to keep a record of personal information and the specific purpose thereof[371] as well as the third parties to whom personal information was disclosed, the date and the purpose of disclosure.[372] These records should be kept for at least one year after the data has been processed.

The act does not determine the nature or format of a record that the data controller is supposed to keep. Since the essence of the ECT touches on the development of information technology and electronic communications, it is submitted that a record can be recorded information in any form or medium.[373]

4.1.4 Obsolete data

The ECT compels a data controller who subscribes to the provisions to delete or destroy all personal information that has become obsolete.[374] A comparable requirement is found in the second half of article 6(1)(d) of the general directive. According to this requirement data which are inaccurate or incomplete should be erased or rectified (considering the purposes of collection and processing).

[371] Section 51(5)
[372] Section 51(7)
[373] A data subject's right to access of personal data is not discussed here, since it resorts under the ambit of the Promotion of Access to Information Act (2 of 2000).

4.1.5 Accuracy

The Directive requires that personal data must be accurate and up to date.[375] The ECT does not mention any prerequisite that a data controller should take reasonable steps to ensure that data is accurate.

4.1.6 Other differences

The biggest difference is found in the obligatory or voluntary nature of these documents. The general directive is a document with authority compelling Member States to enact corresponding legislation. The Member States are also under the obligation to ensure that the provisions are upheld nationally.[376] The ECT, on the other side, does not compel data controllers to comply with the provisions of the act. This is stated clearly in section 50.[377]

Another difference is that the general directive makes provision for the establishment of a supervisory authority in each Member State. Article 28 puts emphasis on the fact that "[e]ach Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them." The article continues and describes the powers and responsibilities of such authorities. The ECT does not provide for the establishment of any similar authority to oversee that the privacy provisions are adhered to. A reason may be that data controllers are not under the obligation to subscribe to the principles. The ECT makes provision for the appointment of cyber inspectors[378] but their duties are wider than to see to it that personal information is protected. These cyber inspectors are required by law to monitor and inspect web sites, cryptography and authentication service providers and perform audits relating to critical databases.[379]

---

[374] Section 51(8)
[375] Article 6(1)(c)
[376] Article 6(2) of the general directive.
[377] See chapter 5 (3.2.1)
[378] Chapter XII of the ECT.
[379] Section 81

The last significant difference mentioned here is that the Directive supplies a general provision that personal data must be processed fairly and lawfully.[380] Such a safeguarding prerequisite does not exist in the ECT.

4.2 Directive 2002/58/EC

This Directive was adopted to embody principles that are connected to the rapid development of technology. It can be regarded as a supplementary to the general directive discussed above. Article 3 of this directive confirms this purpose: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community".

The provisions in this directive involve particular subjects, such as the confidentiality of communications, the processing of traffic data and other technical features. The ECT does not address these issues in so much detail and a rational comparison is not possible.[381] The ECT is a piece of legislation that concentrates on general topics and it does not direct complex issues.

This supplementary directive of the European Union is supposed to be adopted into national law by 31 October 2003.

5. Conclusion

South African law makes provision for the protection of personal information under the principles of the right to privacy. The legislature has gone further and has granted protection to information in this technological society by compiling the Electronic Communications and Transactions Act[382] that was adopted in August 2002.

This act displays provisions that are analogous to the Directives of the European Union and compares well with the requirements of a technological society. The act addresses

[380] Article 6(1)(a)

[381] The issue of confidentiality of communications in article 5 of the Directive may be significant when one consider the relevant parts in the Interception and Monitoring Prohibition Act (27 of 1992).

the most significant aspects regarding electronic communications and the protection of information although one may regret the fact that compliance with the provisions of data protection is voluntary.

The act is, however, a step in the right direction and South Africa has acceptable data protection provisions in place that most probably will satisfy the main trading partners of the country.

[382] Act 25 of 2002

CHAPTER SIX
PERSONAL ELECTRONIC DATA PROTECTION: UN GUIDELINES AND OTHER DOCUMENTS

1. Introduction

Since the Internet shows very little consideration for national borders, solutions for problems arising from the use of the Internet can without much difficulty be sought on international level. Therefore, international bodies such as the United Nations have a very important role to play.

2. UNCITRAL

The United Nations Commission on International Trade Law (UNCITRAL), the UN body concerned with e-commerce, is mainly engaged in the issues of computer evidence, contracts and digital signatures and great progress is made on these topics.[383]

The Commission has for some time been working on the legal consequences of the development of e-commerce. In 1996 the Model Law on Electronic Commerce was finalised and adopted, with an additional article adopted in 1998. The Model Law was adopted to serve as a more effective tool for States that modernises their legislation. Some of the main objects were to remove uncertainty as to the legal effect and validity of paperless messages and to create a more secure legal environment for electronic commerce.

The Model Law does not in particular refer to the protection of data or privacy principles that refer to electronic commerce.

[383] See www.bmck.com/ecommerce/uncitral-t.htm

3. OECD Guidelines

In 1978 the Organisation for Economic Cooperation and Development (OECD)[384] convened a group of experts to study developments in different countries and to present guidelines that might form a consensus of privacy issues, especially in America, but which can serve as a guide for other countries as well.

In 1980 the OECD published its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (OECD Guidelines).[385] The Guidelines are in the language of recommendation rather than obligation.[386] The character of the Guidelines is formulated in guideline 6: ”These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties."

The eight main points of the guidelines concern the principles of limitation on collection; data quality; specification of purpose; limitation of use; security and safeguards; openness; individual participation; and accountability.

The general opinion is presently that the principles of the OECD Guidelines are outdated[387] and should be replaced by a set of standards that is more applicable to current situations.

In October 1998 the OECD convened a conference with the theme “A Borderless World: Realising the potential of Global Commerce” in Ottawa, Canada.[388] The protection of personal information, cross-border flow of information and Internet privacy were some of

[384] The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated thereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

[385] Available at www.ensi.net/odo/akty/Guidelines.htm

[386] Michael 1994:40

[387] See Winn 2000:260 for a detailed discussion on the shortcomings of the OECD Guidelines.

[388] www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec%2898%2914-final.

the themes that were tabled at the conference. The preliminary documents that paved the way for the enactment of the ECT were based on some of these themes.

At the Ottawa conference the participants agreed that users must gain confidence in the digital marketplace. It was accepted that governments have fundamental responsibilities to provide such confidence and ensure continued confidence in the physical marketplace. The role of the private sector was also highlighted in areas were actions to promote growth and use of electronic commerce were important.[389]

Representatives of trade unions and other social interest groups considered it of vital importance that existing concerns in the areas of privacy of consumer an employees, consumer protection (security of payment, reliability of business, getting redress etc.) and the distribution of offensive and harmful content are sufficiently resolved.[390]

The Governments of OECD Member Countries, through their representatives, adopted three declarations to commit themselves to the responsibility they have. These three declarations are: the Declaration on the Protection of Privacy on Global Networks, the Declaration on Consumer Protection in the context of Electronic Commerce and the Declaration on Authentication for Electronic Commerce.

With the Declaration on the Protection of Privacy on Global Networks the representatives reaffirmed the objectives set forth in the Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980. They declared that they will take the necessary steps to implement OECD Privacy Guidelines and in particular the adoption of privacy policies, the notification of privacy policies to users and effective enforcement mechanisms.[391]

The OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" were adopted as a recommendation of the OECD Council at its 1037th session on 25 July 2002.[392]

---

[389] Conference Conclusions of the Ottawa conference October 1998 p.5.
[390] Conference Conclusions of the Ottawa conference October 1998 p.10.
[391] Declaration on the Protection of Privacy on Global Networks (Annexure 1 to the Conference Conclusions p. 14.)
[392] This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL]. The Recommendation is available at www.uerj.br/dinfo/virtual/download/manual_oecd.pdf

4. Council of Europe

In 1980, the Committee of Ministers of the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In contrast to the OECD guidelines, which are voluntary in nature, the Council of Europe Convention is a contractual commitment of the ratifying States and is legally binding. This convention formulates a number of basic principles representing minimum standards that must be incorporated in the legislation of the contracting States. Although similar to the OECD guidelines, these principles are narrower and more specific.

5. Conclusion

The only platform from which one can regulate Internet-related problems, such as Internet crime and data protection, is international bodies such as the United Nations.

This objective is addressed regularly at conferences, conventions and summits that are attended by the majority of first world countries as well as developing third world countries.

The advantage of such gatherings is that a forum is established where every country can contribute towards international policy. The success of such conventions, however, lies at the countries themselves. The documents and recommendations compiled must be enforced nationally in order to give authority to the principles set out in these documents.

Because of the borderless nature of the Internet, this global network and the problems associated with it can only be regulated on an international level.

CHAPTER SEVEN
CONCLUSION AND RECOMMENDATIONS

1. Conclusion

Data protection is a very important aspect internationally which has a huge influence on the use of the Internet by individuals. Although not all of them were mentioned, most first world and developing countries have legislation in place that regulates this issue or part thereof. With the enactment of the ECT, South Africa joined this group of countries.

In most countries considered, the definition for “personal information” is extensive enough to include commercial information. It is also submitted that the definition provided in the ECT is also sufficient to protect commercial information. The protection granted to privacy and personal information can, therefore, be extended within the ambit of the provided definitions to also include commercial information.

Europe's approach, which is very strict and prescriptive, is submitted as the preferable alternative. The Directive establishes an obligation on European level. On an international level, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 as well as the OECD Guidelines for the Security of Information Systems of 26 November 1992 and the declarations adopted at eh Ottawa conference contain general principles for safety measures.

In the light of all these events, the Americans still seem to favour the system of self-regulation. This system does not provide the same sense of security among individuals as legislative measures do. The reason being that sanctions go hand in hand with legislation and the certainty of punishment. However, it compels businesses to reassure their customers through thorough privacy policies and adherence to it. This proves to give some businesses a professional advantage. When enforcement authorities exist

and they have a well-defined mandate, the self-regulatory system may prove to be successful.

The defence that the Internet is a technologically superior field that develops rapidly, is noted, but legislation can still be enacted to protect individuals' personal information which includes commercial information. Measures such as these normally include basic principles that stay valid amid changing circumstances.

It is true that the ECT represents a huge leap for South Africa in the area of commercial law and especially electronic commercial or Internet law. It covers a multitude of aspects of which only a few were discussed in this dissertation. While violations of privacy are not criminal offences, the ECT creates offences where unauthorised access to, interception of and interference with data are punishable.

2. Recommendations for data protection in the South African context.

When one examines the ECT, one cannot neglect to point out areas of concern. The ECT creates criminal offences which may prove to be a much greater responsibility that existing law enforcement agencies can handle. The enforcement mechanism in other countries is usually given to either a private or separate public regulatory body (in Europe this is usually the task of the Data Protection Commissioner who can investigate complaints relating to data protection and who has the right to institute criminal or civil proceedings in this regard and in the United States the FTC fulfils this function).

Another area of concern is that the ECT merely sets out preferred ways of conduct when businesses process personal information. In many instances no obligation rests on an organisation to comply with set ways of conduct.

In light of the deficiencies of the Act, it is suggested that concerned business begin to create their own industry codes to ensure that they or their industries comply with international best practice. These codes should contain the principles as set out in the

Act and which will cater for their respective industry needs. When these are created, a private regulatory body can oversee the enforcement of the industry-specific codes to ensure that the principles are not merely being played lip-service. In the US, Europe and Australia these types of Codes of Conduct have proved very valuable in the protection of data subjects' privacy.[393]

One must still keep in mind that laws that make privacy violations and unauthorised intrusions illegal, cannot prevent violations; they can only deter intrusions. Therefore, a system with the appearance of self-regulation in conjunction with the principles set forth in the ECT, can provide an industry that enforces good data privacy principles.

[393] Heyink 2002

SUMMARY

The purpose of this study was to investigate whether the commercial information of an individual is adequately protected when the individual makes use of electronic communications. This issue was addressed in two parts, namely the unauthorised access to commercial information, incorporating internet crime and the protection of personal electronic data.

Under the first part two levels of access were identified. The first level dealt with the protection of information from misuse and in this section computer crime, relevant to the information of an individual, received attention. The concern of identity theft was investigated and several solutions were proposed that is available at present, including different methods of payment.

The second level of the first part looked into the protection of information from third parties (who do not have permission for access). In this section cookies, spam, hacking and data mining were briefly taken into account.

The second part of this study observed the protection of information that is granted to citizens of different countries under their appropriate legislation and common law principles. The principles governing the protection of privacy in the United States of America and the United Kingdom as well as in South Africa were taken into account. In particular the directives of the European Union on this theme received consideration.

Throughout this study, reference has been made to the newly enacted Electronic Communications and Transaction Act (25 of 2002). Furthermore, a comparison was drawn to explore how the principles protecting personal and commercial information in the mentioned act weighed up against or contrasted with the European Union's directives.

In addition, this study regarded the developments on international level and in particular the activities of the Organisation for Economic Co-operation and Development (OECD), other United Nations projects and activities by the Council of Europe.

OPSOMMING

Die doel van hierdie studie was om te ondersoek of die kommersiële inligting van ‘n individu genoegsame beskerming geniet wanneer die individu gebruik maak van elektroniese kommunikasie. Die aspek is aangespreek in twee dele, naamlik die ongemagtigde toegang tot kommersiële inligting, wat insluit internetmisdaad, en die beskerming van persoonlike elektroniese data.

Onder die eerste deel is twee vlakke van toegang geïdentifiseer. Die eerste vlak het gehandel met die beskerming van inligting teen wangebruik en in hierdie deel het rekenaarmisdaad, waar dit van toepassing is op die inligting van ‘n individu, aandag geniet. Die aangeleentheid van identiteitsdiefstal is ondersoek en ‘n aantal oplossings wat tans beskikbaar is, is voorgestel, insluitende verskillende betaalwyses.

Die tweede vlak van die eerste deel het gehandel met die beskerming van inligting teen derdes (wat nie toestemming het om toegang te verkry nie). In hierdie deel is koekies, gemorspos, “hacking” en data-ontginning kortliks oorweeg.

Die tweede deel van die studie het die beskerming van inligting wat gebied word aan burgers van verskillende lande, volgens wetgewing en gemenereg, in aanmerking geneem. The beginsels wat die beskerming van privaatheid in die Verenigde State van Amerika, die Verenigde Koninkryk en Suid-Afrika beheer, is in oënskou geneem. In die besonder is die direktiewe van die Europese Unie oor hierdie aangeleentheid oorweeg.

Regdeur die studie is daar verwys na die onlangse Wet of Elektroniese Kommunikasie en Transaksies (25 van 2002). ‘n Vergelyking is voorts getref om uit te vind hoe die beginsels in die genoemde wet wat persoonlike en kommersiële inligting beskerm, opweeg teen, of verskil van die direktiewe van die Europese Unie.

Verder het die studie die ontwikkelings op internasionale vlak en in die besonder aktiwiteite van die Organisasie vir Ekonomiese Samewerking en Ontwikkeling (OECD), ander projekte van die Verenigde Nasies en aktiwiteite van die Europese Raad in aanmerking geneem.

BIBLIOGRAPHY

ANDREWS, EL
1998. European law aims to protect privacy of personal data. 26 October. www.nytimes.com/library/tech/98/10/biztech/articles/26privacy.html.

ANONYMOUS
2003. Survey shows steep rise in identity theft. http://www.sfgate.com/cgi-bin/article.cgi?file= /chronicle/archive/2003/07/22/BU279349.DTL&type=business.

ANONYMOUS
1994. Electronic Money. *The Economist* 26 November p211.

BAASE, S
1997. *A Gift of Fire: Social, Legal and Ethical Issues in Computing*. New Jersey: Prentice Hall.

BIDOLI, M
2001. Terror attacks may cost South Africans their freedom. *Financial Mail* 12 p36.

BOUKHARI, S
1998. Cybersnoopers on the prowl. *UNESCO Courier* September p44.

BURCHELL, J
1998. *Personality Rights and Freedom of Expression.* Cape Town: Juta & Company Ltd.

BURCHELL, J and MILTON, J
1997. *Principles of Criminal Law.* Second edition. Cape Town: Juta & Company Ltd.

BUYS, R (ed)
2000. *Cyberlaw @ SA: The Law of the Internet in South Africa.* Pretoria: Van Schaik Publishers.

CHASKALSON, A *et al*
1999. *Constitutional Law of South Africa.* Revision Service 5. Cape Town: Juta & Company.

COHEN, A
2000. Spies among us. *Time* 156(5) p 37.

CRADDOCK, A
1998. June, 25. www.wired.com/news/politics/0,1283,13256,00.html.

CRANOR, LF
1999. Internet Privacy. *Communications of the ACM* 42(2) p29.

DAVIDSON, T
1998. For your eyes only. *Charter* 69(3) p48.

DAVIES, S
1998. Europe to U.S.: No privacy, no trade. May. www.wired.com/wired/6.05/europe.html.

DEVENISH, GE
1999. *A Commentary on the South African Bill of Rights.* Durban: Butterworths.

DUNLOP, C and KLING, R
1991. *Computerization and Controversy: Value conflicts and social choices*. Boston: Academic Press.

EBERSöHN, GJ
2002. *Copyright and Trade Mark infringements: The Digital Evolution*. LL.D. (UFS).

EBERSöHN, GJ
2001. *Internet related commercial crimes.* LL.M (UFS).

EIJK, MJT
2000. Klant in het Web: Privacywaarborgen voor Internettoegang. June. www.cbp web.nl/ documenten/av_17_Klant_in_het_web.htm.

ELS, F
2000. Die oë wat loer, raak al hoe meer. *Finansies & Tegniek* 52(10) p31.

FLOOR, J
2002. Data doesn't travel well. *Finance Week* March 1 p63.

FRIEDMAN, MS and BISSINGER, K
1998. Infojacking: Crimes on the Information Superhighway! www.sgrm.com/art15.htm.

GLAVE, J
1998. Survey: Privacy Laws Common. www.wired.com/news/politics/0,1283,15428,00.html.

GAHTAN, A
1997. Financial service in an Electronic Age: Some emerging legal issues. June. www.gahtan.com/alan/articles/ibank-b.htm.

HEYINK, M
2002. Privacy: The concept and emerging regulation. 2 April. www.itweb.co.za.

JANSEN, FA
1998. *Data Privacy: An overview of international legislation and the position in South Africa.* (UFS).

JANSEN JH
2002. A New Era for e-commerce in South Africa. *De Rebus* October p16.

KLOPPER, HB
1986. *Die beskerming van kredietwaardigheid in die Suid-Afrikaanse reg*. LL.D (UOFS).

KORNOWSKI, J
1997. Get ready to pass the cyber-buck: Following the 'electronic' money. www.lacba.org/lalawyer/tech/ecash.html.

LAW, L *et al*
1996. How to make a mint: the cryptography of anonymous electronic cash. 18 June. http://jya.com/nsamint.htm.

LAWACK-DAVIDS, VA
2001. The Cryptographic Dilemma: Possible approaches to formulating policy in South Africa. *Obiter* 22(1) p1.

LAWACK-DAVIDS, VA
2000. *Aspects of Internet payment instruments*. LL.D (UNISA).

LIIKANEN, E
2003. Cybersecurity and the European Network and Information Security Agency. 11 June. http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/03/293|0|RAPID&1g=EN&display=.

MALKIN AND HAMBRIDGE
1999. *Don't spew*. www.ietf.org/internet-drafts/draft-left-run-spew-08.txt.

McCULLAGH, D
2003. Is privacy making a comeback? 28 July. http://news.com.com/2010-1071_3-5055782html?tag=fd_nc_1.

McLEAN, D
1995. *Privacy and its Invasion*. Westport: Praeger.

McQUOID-MASON, DJ
1978. *The Law of Privacy in South Africa*. Cape Town: Juta & Company Ltd.

MICHAEL, J
1994. *Privacy and Human Rights: an international and comparative study with special reference to developments in information technology.* Dartmouth: UNESCO Publishing.

NAUMOV, V
2003. Legal Issues in Personal Data Protection on the Russian Internet. 4 February. www.russianlaw.net/english/ae04.htm.

NEETHLING, J *et al*
2002. *Law of Delict.* Fourth edition. Durban: Butterworths.

NEETHLING, J
1999. *LAWSA*. Personality Infringement. First Reissue vol 20(1). Durban: Butterworths.

NEETHLING, J
1998. *Persoonlikheidsreg.* Fourth edition. Durban: Butterworths.

NEETHLING, J
1992. Computers and private-law legal remedies for the protection of privacy, trade secrets, patents and copyright. *Codicillus* 33(1) p4.

NEETHLING, J
1990. Die reg op die verdienvermoë en die reg op die korrekte inligting as selfstandige subjektiewe regte. *Journal of Contemporary Roman-Dutch Law* 53 p101.

OBRINGER, LA
2002. How Identity theft works. Http://computer.howstuffworks.com/identity-theft9.htm.

PABRAI, UOA
2002. Improve user trust on the Web. *E-Business Advisor* 20(40) p30.

RAMASASTRY, A
2003. Third Party Data Monitoring and Collection on the Internet. 4 June. http://writ.corporate.findlaw.com/ramasastry/20030604.html.

RASCH, MD
1996. Criminal Law and the Internet. http://cla.org/RuhBook/chp11.htm.

RENS, A
2003. Approach with Caution. *De Rebus* June p23.

ROGERS, WVH
1989. *Winfield and Jolowicz on Tort*. Thirteenth edition. London: Sweet & Maxwell.

ROOS, A
1990. Data privacy: the American experience. *Tydskrif vir Suid-Afrikaanse Reg* 2 p264.

ROOS, A
1990. Data Privacy: the American experience (continued). *Tydskrif vir Suid-Afrikaanse Reg* 3 p477.

ROSENOER, J
1995. The Privacy Directive. 12 August. www.cyberlaw.com/cylw0895.html.

RYRIE, T
2000. Monitor Wizards. *Charter* 71(8) p42.

SCHJOLBERG, S
2003. The legal framework - unauthorized access to computer systems. 7 April. www.mosstingrett.no/info/legal.html.

SCOTT, GH
1995. *Mind your own business: The battle for Personal Privacy.* New York: Insight Books.

SIEBER, U
1998. Legal Aspects of Computer-Related Crime in the Information Society. www.cybercrimes.net/International/IntLinks.html.

SING, D and BAYAT, MS
1992. Computer technology and information privacy rights of the individual. *Tydskrif vir Regswetenskap* 17(1) p80.

SNYMAN, CR
2002. *Criminal Law.* Fourth edition. Durban: Butterworths.

STRAUSS, SA (ed)
1988. *Huldigingsbundel vir WA Joubert.* Durban: Butterworths.

VAN DER MERWE, DP
2003. Computer crime – recent national and international developments. *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 66 p30.

VAN DER MERWE, DP
2000. *Computers and the Law.* Second edition. Cape Town: Juta & Company Ltd.

VAN DER MERWE, DP
1999. Die regsimplikasies van elektroniese handeldryf ("e-commerce") met besondere verwysing na die bewysreg. *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* 62 p 226.

VAN DER MERWE, DP
1998. *LAWSA*. Computers. First Reissue vol 5(3). Durban: Butterworths.

VAN DER WALT, AJ and PIENAAR, GJ
2002. *Introduction to the Law of Property.* Fourth edition. Cape Town: Juta & Company.

WATSON, J
2001. Privacy online. *SA Computer Magazine* 9(7) p54.

WESSELS, J
2003. Privacy en recht. www.internetprivacy.nl/recht.html.

WESTIN,
1968. *Privacy and Freedom*. New York: Athenum.

WILHELMSSON, T *et al*
2001. *Consumer Law in the Information Society.* London: Kluwer Law International.

WINN, JK and WRATHALL, JR
2000. Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data. *Business Lawyer* 56(1) (November) p213.

WRIGHT, B
2003. Act on ECT. *SA Computer Magazine* 11(2) p24.

WRIGHT, B
2002. Piracy vs Privacy. *SA Computer Magazine* 10(16) p43.

WRIGHT, B
2001. Cyberlaw. *SA Computer Magazine* 9(9) p36.

TABLE OF OTHER DOCUMENTS, REPORTS AND CONVENTIONS

SOUTH AFRICA

SOUTH AFRICAN LAW REFORM COMMISSION
2000. *Computer-related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects.* Discussion Paper 99. Project 108.

SOUTH AFRICAN LAW REFORM COMMISSION
1998. *Computer-related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects.* Issue Paper. Project 108.

DEPARTMENT OF COMMUNICATIONS
2000. Green Paper on E-commerce. www.polity.org.za/govdocs/green_papers/greenpaper/

EUROPE

COUNCIL OF EUROPE
1989. Recommendation no. R(89) 9 on Computer-related crime. http://cm.coe.int /ta/rec/1989 /89r9.htm.

COUNCIL OF EUROPE
1995. Recommendation no. R (95) 13 Concerning Problems of Criminal Procedure Law connected with Information Technology.

COUNCIL OF EUROPE
2001. Convention on Cybercrime. http://conventions.coe.int/treaty/EN/projets/Final Cybercrime.htm.

EUROPEAN UNION
1995. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281/31 of 23.11.1995. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEX numdoc&1g=EN&numdoc=31995L0046&model=guichett.

EUROPEAN UNION
2002. Fifth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the year 2000. Part II. 6 March. 10557/02/EN final. WP 54.

EUROPEAN UNION
2002. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. 12 July. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&1g=

EN&numdoc=32002L0058&model=guichett.

NETHERLANDS
2000. Annual Report of the College Bescherming Persoonsgegevens. www.cbpweb.nl/structuur/pag_handel.htm.

UNITED NATIONS

OECD
2002. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. www.uerj.br/dinfo/virtual/download/manual_oecd.pdf.

OECD
1998. A Borderless World: Realising the potential of Global Commerce. www.ottawaoecdconference.org /english/homepage.html.

OECD
1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. www.ensi.net/odo/akty/Guidelines.htm.

UNITED NATIONS
1990. Manual on the prevention and control of computer-related crime. www.uncjin.org/Documents/EighthCongress.html#congress

UNCITRAL
1996. Model Law on Electronic Commerce with Guide to Enactment (with additional article 5 bis as adopted in 1998). www.uncitral.org/english/texts/electcom/ml-ecomm.htm.

OTHER INTERNATIONAL ORGANISATIONS

CONSUMERS INTERNATIONAL
2001. Privacy@net: An International Comparative Study of electronic commerce and data protection. January. http://www.consumersinternational.org/publications/searchdocument.asp?PubID=30&regionid=135&langid=1.

TABLE OF CASES

Canada

R v Stewart 1988 1 S.C.R. 963

South Africa

Blower v Van Noorden 1909 TS 890

Case v Minister of Safety and Security 1996 3 SA 617 CC
Minister of Justice v Hofmeyr 1993 3 SA 131 A

National Media Ltd and Another v Jooste 1996 3 SA 262 SCA

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 3 SA 244 C

R v Umfaan 1908 T.S 62

S v A 1971 2 SA 293 T
S v Bailey 1981 4 SA 187 W
S v Graham 1975 3 SA 569 A
S v Harper 1981 2 SA 368 D
S v I 1976 1 SA 781 RA
S v Kotze 1965 1 SA 118 A
S v Lawrence 1954 2 SA 408 K
S v Meyeza 1962 3 SA 386 N
S v Mintoor 1996 1 SACR 514 C
S v Ndhlovu 1963 1 SA 926 T
S v Ngobeza 1992 1 SASV 610 T
Standard Bank Investment Corporation Ltd v Competition Commission and Others; Liberty Life Association of Africa Ltd v Competition Commission and Others 2000 2 SA 797 SCA

Universiteit van Pretoria v Tommie Meyer Films (Edms)Bpk 1979 1 SA 441 A

Video Parktown North (Pty) Ltd v Paramount Pictures Corporation; Video Parktown North (Pty) Ltd v Shelburne Associates and Others; Video Parktown North (Pty) Ltd v Century Associates and Others 1986 2 SA 623 T

United Kingdom

Malone v Metropolitan Police Commissioner 1979 Ch. 344

United States of America

CompuServe, Inc. v Patterson 89 F.3d 1257 (6th Cir. 1996)

In Re Pharmatrak, Inc. Privacy Litigation Available at http://caselaw.lp.findlaw.com /scripts/getcase.pl?court=1st&navby=case&no=022138&exact=1

Griswold v Connecticut 381 US 186

Hill v Gateway 2000, Inc. 105 F.3d 1147 (7th Cir. 1997)
Hotmail Corp. v Van$ Money Pie, Inc. 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998)

International News Service v Associated Press 248 U.S. 215 (1918)

Katz v United States 389 US 347 (1967)

McVeigh v Cohen 983F Supp 215 (D) DC 1998

Nixon v Administrator of General Services 433 US 425 (1970)

Paul v Davis 424 US 693 at 712 (1976)
ProCD, Inc v Zeidenberg 86 F.3d 1447, (7th Cir. 1996) (Available at http://laws.findlaw.com/7th/ 961139.html)

Roe v Wade 410 US 113

United States v Miller 425 US 435 (1976)

TABLE OF LEGISLATION

Austria

Data Protection Act (Datenschutzgesetz 2000, BGB1. I Nr 165/1999 of 17.08.1999)

Denmark

Act on Processing of Personal Data, Act No. 429 of 31 May 2000

Finland

Personal Data Act, 523/1999

Germany

Federal Data Protection Act (Bundesdatenschutzgesetz) (20 December 1990, Federal Law Gazette I 1990 p. 2954 with amendments)

Greece

Law on the Protection of the Individual with regard to the processing of personal data, law 2472/97 (As amended by Laws 2819/2000 (Official Gazette 84 A 15.03.2000) and 2915/2001(Official Gazette 109 A 19.05.2001)

Ireland

Data Protection (Amendment) Act of 2003

Italy

Data Protection Act no. 675 of 31 December 1996.

Netherlands

Dutch Data Protection Act

Portugal

Data Protection Act, Law 67/98 of 26 October.

Sweden

Personal Data Act, 1998:204

Spain

Organic Law No 15/1999 *on the protection of personal data*

South Africa

Promotion of Access to Information Act 2 of 2000
Electronic Communications and Transactions Act 25 of 2002
Interception and Monitoring Prohibition Act 127 of 1992
South African Trespass Act 6 of 1959

United Kingdom

Computer Misuse Act of 1990 (c. 18).
Theft Act of 1968
Data Protection Act of 1998

United States of America

Communications Assistance for Law Enforcement Act 47 U.S.C. § 1001-1027
Electronic Communications Privacy Act of 1986 18 U.S.C. § 1028 (Supp. IV 1998)
Fair Credit Reporting Act 15 United States Code §
Gramm-Leach-Bliley Act 15 U.S.C. § 6801
Identity Theft and Assumption Deterrence Act 18 U.S.C. §1028
Online Privacy and Policy Disclosure Act of 2003 U.S.C. §552a
Privacy Act 5 U.S.C. § 552a
Uniform Trade Secrets Act 14 U.L.A. 433 (1990 & Supp. 2000)
USA PATRIOT Act Public law 107-56 (107th Congress)

LIST OF KEY TERMS AND RELEVANT DEFINITIONS

Cookies

Cookies (or “little brothers” as they are sometimes called) are HTTP headers that consist of a text-only string. The string is usually a set of random-looking letters long enough to be unique to every user. The cookie is sent from the server of the web site the user accessed the first time and is saved on the user's hard drive. When the user accesses that site again, a copy of the cookie is sent with the request to that site. In this way the remote server knows who the user is and that he or she visited the site before and it can keep track of items purchased.[394]

Cyberspace

“‘Cyber’ is the prefix used to indicate Internet-related entities. The realm of the Internet is often referred to as ‘cyberspace’.”[395]

E-commerce

E-commerce or electronic commerce is the process of doing commercial transactions electronically.[396]

ECT

This abbreviation is used when referred to the Electronic Communications and Transactions Act (Act 25 of 2002) that commence on 20 August 2002.

E-mail

E-mail or electronic mail is messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses (mailing list).[397]

Hacking and cracking

The unauthorised access to computers is commonly known as “hacking”. “Hacker” is “a digital-era term often applied to those interested in techniques for circumventing

[394] Buys 2000:385; FTC privacy policy, available at www.ftc.gov/ftc/privacy.htm
[395] Ebersöhn 2002:10
[396] Buys 2000:462
[397] Buys 2000:462

protections of computers and computer data from unauthorized access. The so-called hacker community includes serious computer-science scholars conducting research on protection techniques, computer buffs intrigued by the challenge of trying to circumvent access-limiting devices or perhaps hoping to promote security by exposing flaws in protection techniques, mischief-makers interested in disrupting computer operations, and thieves…"[398]

While hackers normally do not have malicious intentions, crackers are perpetrators who do not intend to simply gain entry to computer networks, but they have ulterior motives. They can bring computer systems to a halt or they will make copies of sensitive information for use in an unlawful manner.

HTTP

HTTP is an abbreviation for Hyper Text Transfer Protocol. This is the protocol for moving hypertext files across the Internet. In order to do this there has to be an HTTP client programme at one end and an HTTP server programme at the other end. HTTP is the most important protocol used in the World Wide Web.

Identity theft

Identity theft is a concept that is exactly expressed by its description. Although it is not "theft" in the common law sense, identity theft can range from unauthorised use of your credit card to someone creating a "duplicate you" complete with your birthday and identity number, leaving you with a pile of unpaid bills. This kind of theft tarnishes your credit record, and results in the loss of credit, employment and can even lead to criminal charges for a crime you did not commit.

Internet

The Internet is a collection of interconnected computer networks that covers the entire world. The Internet links personal computers by means of servers, which run specialised operating systems and applications designed for servicing a network environment.[399] The Electronic Communications and Transactions Act 25 of 2002 defines "Internet" in section 1 as "the interconnected system of networks that connects computes around the world using the TCP/IP and includes future versions thereof".

[398] As quoted in Ebersöhn 2002:11

ISOC-ZA prefers the definition: "Internet" means the global network of interconnected networks that use the TCP/IP protocol suite.

Information crime

Information crime is a part of computer crime that can be committed over the Internet. This occurrence of the crime deals with issues relating to information and especially the personal or private information of person.

Internet Service Provider (ISP)

An Internet Service Provider can be a business that delivers access to the Internet, usually for a monthly fee. M-Web, UUNET and Netco are examples of established ISPs but there are thousands of smaller ones all around the world. An ISP can also be a business that provides Internet services such as web sites or web site development.[400]

IP address

Every machine on the Internet has a unique identifying number, called an IP Address. The IP stands for Internet Protocol, which is the language that computers use to communicate over the Internet. A protocol is the pre-defined way that someone who wants to use a service talks with that service. The "someone" could be a person, but more often it is a computer program like a Web browser. A typical IP address looks like this: 216.27.61.137.[401]

Login

To log into a network a password is normally used. This password is referred to as a “login”.

Password

A password is a code used to gain access to a locked system. Good passwords contain letters and non-letters and are not simple combinations, such as virute7. A good password may be: Hot$1-6.

---

[399] Ebersöhn 2002:12
[400] Buys 2000:464
[401] http://computer.howstuffworks.com/internet-infrastructure3.htm

PC

PC is the abbreviation for personal computer. A PC is normally not part of a network, but is used in homes where it is from time to time connected to the Internet through a dial-up connection.

Packet sniffing

Information is "broken up" and sent over the Internet in the form of smaller parts, called data packets. When these packets travel across the Internet, they can be intercepted, a copy of the original can be made and the original packet can again be sent on its way. This is known as “packet sniffing”.

Spam

Spamming refers to the bulk sending of unsolicited e-mail advertisements to huge numbers of Internet users.

Surf

“To surf the Internet means to browse or explore a network or the World Wide Web to find places of interest, usually without a specific goal in mind. It is analogous to channel surfing with a TV remote control.”[402]

Trojan horse

A Trojan horse is an insidious and usually illegal computer programme that masquerades as a programme that is useful, fun or otherwise desirable for users to download to their system. Once the programme is downloaded, it performs a destructive act.[403]

User

A user in the context of this dissertation is a person who uses computer software or the Internet.

[402] Buys 2000:467

Virus

A virus is an insidious piece of computer code written to damage systems. Viruses can be hidden in executable programme files posted online.[404]

Virus-planting

Virus-planting is the introduction of a computer virus into a computer or network.

Web site

A web site is a "collection of Web pages published on the Web by an individual or organization… Most Web pages are in the form of 'hypertext'; that is, they contain annotated references, or 'hyperlinks' to other Web pages."[405]

World Wide Web (WWW)

The World Wide Web is a distributed hypertext system invented by Tim Berners-Lee on a NeXT computer. It is now one of the most popular services offered on the Internet. Web pages are viewed using browsing software such as Netscape Navigator, Sun Microsystems Hot Java or Microsoft Internet Explorer.[406]

---

[403] Buys 2000:468
[404] Buys 2000:468
[405] Ebersöhn 2002:17
[406] Buys 2000:469

KEY TERMS

Computer crime
Cookies
Data protection
Electronic Communications and Transactions Act (25 of 2002) (ECT)
Electronic payment
Hacking
Identity theft
Information crime
Internet
Personal information
Privacy
Spam

SLEUTELWOORDE

Elektroniese betaalwyses
Identiteitsdiefstal
Inligtingsmisdaad
Internet
Persoonlike inligting
Privaatheid
Rekenaarmisdaad
Wet op Elektroniese Kommunikasie en Transaksies (25 van 2002)

SUMMARY

The purpose of this study was to investigate whether the commercial information of an individual is adequately protected when the individual makes use of electronic communications. This issue was addressed in two parts, namely the unauthorised access to commercial information, incorporating internet crime and the protection of personal electronic data.

Under the first part two levels of access were identified. The first level dealt with the protection of information from misuse and in this section computer crime, relevant to the information of an individual, received attention. The concern of identity theft was investigated and several solutions were proposed that is available at present, including different methods of payment.

The second level of the first part looked into the protection of information from third parties (who do not have permission for access). In this section cookies, spam, hacking and data mining were briefly taken into account.

The second part of this study observed the protection of information that is granted to citizens of different countries under their appropriate legislation and common law principles. The principles governing the protection of privacy in the United States of America and the United Kingdom as well as in South Africa were taken into account. In particular the directives of the European Union on this theme received consideration.

Throughout this study, reference has been made to the newly enacted Electronic Communications and Transaction Act (25 of 2002). Furthermore, a comparison was drawn to explore how the principles protecting personal and commercial information in the mentioned act weighed up against or contrasted with the European Union's directives.

In addition, this study regarded the developments on international level and in particular the activities of the Organisation for Economic Co-operation and Development (OECD), other United Nations projects and activities by the Council of Europe.

OPSOMMING

Die doel van hierdie studie was om te ondersoek of die kommersiële inligting van ‘n individu genoegsame beskerming geniet wanneer die individu gebruik maak van elektroniese kommunikasie. Die aspek is aangespreek in twee dele, naamlik die ongemagtigde toegang tot kommersiële inligting, wat insluit internetmisdaad, en die beskerming van persoonlike elektroniese data.

Onder die eerste deel is twee vlakke van toegang geïdentifiseer. Die eerste vlak het gehandel met die beskerming van inligting teen wangebruik en in hierdie deel het rekenaarmisdaad, waar dit van toepassing is op die inligting van ‘n individu, aandag geniet. Die aangeleentheid van identiteitsdiefstal is ondersoek en ‘n aantal oplossings wat tans beskikbaar is, is voorgestel, insluitende verskillende betaalwyses.

Die tweede vlak van die eerste deel het gehandel met die beskerming van inligting teen derdes (wat nie toestemming het om toegang te verkry nie). In hierdie deel is koekies, gemorspos, “hacking” en data-ontginning kortliks oorweeg.

Die tweede deel van die studie het die beskerming van inligting wat gebied word aan burgers van verskillende lande, volgens wetgewing en gemenereg, in aanmerking geneem. The beginsels wat die beskerming van privaatheid in die Verenigde State van Amerika, die Verenigde Koninkryk en Suid-Afrika beheer, is in oënskou geneem. In die besonder is die direktiewe van die Europese Unie oor hierdie aangeleentheid oorweeg.

Regdeur die studie is daar verwys na die onlangse Wet of Elektroniese Kommunikasie en Transaksies (25 van 2002). ‘n Vergelyking is voorts getref om uit te vind hoe die beginsels in die genoemde wet wat persoonlike en kommersiële inligting beskerm, opweeg teen, of verskil van die direktiewe van die Europese Unie.

Verder het die studie die ontwikkelings op internasionale vlak en in die besonder aktiwiteite van die Organisasie vir Ekonomiese Samewerking en Ontwikkeling (OECD), ander projekte van die Verenigde Nasies en aktiwiteite van die Europese Raad in aanmerking geneem.