SOUTH AFRICAN LAW COMMISSION

DISCUSSION PAPER 99

Project 108

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

Closing date for comment: 2 JULY 2001

ISBN: 0-621-30718-1

INTRODUCTION

The South African Law Commission was established by the South African Law Commission Act, 1973 (Act 19 of 1973).

The members of the Commission are -

Madam Justice Y Mokgoro (Chairperson)
Advocate J J Gauntlett SC
Mr Justice C T Howie
Madam Justice L Mailula
Professor I P Maithufi (Full-time member)
Mr P Mojapelo
Ms Z Seedat

The Secretary is Mr W Henegan. The Commission's offices are on the 12th floor, Sanlam Centre, Corner of Andries and Schoeman Streets, Pretoria.

Correspondence should be addressed to:

The Secretary
South African Law Commission
Private Bag X668
PRETORIA
0001

Telephone: (012) 322-6440
Fax: (012) 320-0936
E-mail: mpalumbo@salawcom.org.za

This document is also available on the Internet at http://www.law.wits.ac.za/salc/salc.html

PREFACE

This discussion paper (which reflects information gathered up to the end of August 2000) was prepared to elicit responses and to serve as a basis for the Commission's deliberations, taking into account any responses received. The views, conclusions and recommendations in this paper are accordingly not to be regarded as the Commission's final views. The discussion paper is published in full so as to provide persons and bodies wishing to comment or make suggestions for the reform of this particular branch of the law with sufficient background information to enable them to place full submissions before the Commission.

The Commission will assume that respondents agree to the Commission quoting from or referring to comments and attributing comments to respondents, unless representations are marked confidential. Respondents should be aware that the Commission may in any event be required to release information contained in representations under the Constitution of the Republic of South Africa, Act 108 of 1996.

Respondents are requested to submit written comments, representations or requests to the Commission by 2 July 2001 at the address appearing on the previous page.

The project leader responsible for this project is Professor D P van der Merwe.

CONTENTS

The page numbers refer to the hard copy and may differ in electronic versions

Page

SOURCES AND CITATION

Battcock

Battcock R **The Computer Misuse Act 1990: 5 years on** Article published electronically on the Internet site of the University of Strathclyde at http://www.strath.ac.uk/Departments/Law/student/PERSONAL/R_BATTCOCK/crime1.html accessed on 10 December 1997.

Charlesworth

Charlesworth A Legislating Against Computer Misuse: The Trials and Trobulations of the UK Computer Misuse Act 1990 1993[4] **Journal of Law and Information Science** Abstract published electronically on the Internet site of the University of Hull at http://www.hull.ac.uk/Hull/Law_Web/complaw/compart/compart1.html accessed on 22 May 2000.

Milton

Milton J R L **South African Criminal Law and Procedure** vol 2 3rd edition Cape Town: Juta 1996

Schmidt

Schmidt C W H **Bewysreg** 3rd edition Durban: Butterworths 1989

Snyman

Snyman C R **Strafreg** 3rd edition Durban: Butterworths 1992

Van der Merwe *et al*

Van der Merwe S E, Morkel D W, Paizes A P, Skeen A St Q **Evidence** Cape Town: Juta 1983

TABLE OF CASES

South Africa

R v Firling 1904 (EDC) 11

R v Heyne 1956 (3(SA 604 (A)

S v Harper 1981 (2) SA 638 (D)

S v Kotze 1965 (1) SA 118 (A)

S v Myeza 1985 (4) SA 30 (T)

S v Ndhlovu 1963 (1) SA 926 (T)

S v Ngobeza and Another 1992 (1) SACR 610 (T)

United Kingdom

R v Strickland, Woods and Bedworth The Times, 18 March 1993

SELECT LEGISLATION

Australia

1914 Crimes Act, 1914

Canada

Criminal Code

Germany

Criminal Code

Singapore

1993 Computer Misuse Act 1993

South Africa

1959 Trespass Act, 1959 (Act 6 of 1959)
1962 Extradition Act, 1962 (Act 67 of 1962)
1977 Criminal Procedure Act, 1977 (Act 51 of 1977)

United Kingdom

1984 Police and Criminal Evidence Act 1984
1985 Interception of Communications Act 1985
1990 Computer Misuse Act 1990

United States of America

Comouter Fraud and Abuse Act, 1986 (US): Title 18 USC

Council of Europe

Draft Convention of Cyber-Crime (Draft No 19)

EXECUTIVE SUMMARY

This investigation focusses on the activities of obtaining unauthorised access to computer data and software applications and of unauthorised modification of computer data and software applications.

Computers are playing an integral part in the functioning of our society. Computers are relied upon to perform functions upon which human life as well as the economic and industrial functioning of society are dependant. The potential danger if computers performing these functions are interfered with is very serious. The Commission therefore proposes that these activities be made subject to criminal sanction.

The activities of obtaining unauthorised access to computer data and software applications and of unauthorised modification of computer data and software applications cannot be dealt satisfactorily with in terms of the present provisions of our criminal law. This indicates that the introduction of new offences by way of legislation should be seriously considered. It is therefore proposed that a "Computer Misuse Act" be developed for this purpose.

The offences that should be contained in such an Act are:

- unauthorised access to applications or data in computer system,
- unauthorised modification of applications or data in computer system,
- development and trafficking in devices or applications primarily used to obtain unauthorised access,
- trafficking in computer passwords, and
- interference with use of computer system.

It is also proposed that a Computer Misuse Act make provision for procedural matters such as search and seizure, admissibility of evidence and jurisdiction.

The Commission's proposals are embodied in a proposed Bill attached to this discusion paper as Annexure A.

CHAPTER 1

1. INTRODUCTION AND BACKGROUND

1.1 During 1997 the Commission decided to include an investigation into computer-related crime in its programme. A project committee was appointed to assist the Commission in this investigation.

1.2 A project to investigate the admissibility of computer generated evidence has already been commenced with by the Commission (Project 95). This project will be proceeded with by the project committee appointed for the project on computer-related crime. The aspects of the admissibility of computer generated evidence relating to criminal matters will be considered in the course of the investigation into computer-related crime. Thereafter the civil aspects of the admissibility of computer generated evidence will be further investigated.

1.3 Computers and the software used on computers are designed to perform a multitude of tasks. These include the storage of information and the performing of a range of functions with such information which can be aimed at, among others, altering the meaning thereof or at producing a totally new product. The ability of computers and software to perform these tasks can naturally be abused for purposes which are unlawful or which are so unacceptable to society that there can be said to be general consensus that they should be unlawful.

1.4 The Commission recognises that the scope of an investigation into computer-related crime is very wide. For this reason the Commission initially set six objectives which it aimed to achieve during the course of the investigation. These are:

- to investigate the criminalisation of unauthorised access to computers as well as the unauthorised modification of computer data and software applications which includes the planting of a virus for example,
- to investigate the possibility of providing for the procedural aspects associated with the investigation and prosecution of the above-mentioned offences,
- to investigate the use of computers to commit offences such as theft and fraud,
- to investigate offences committed by means of the Internet,
- to investigate matters relating to encryption in order to protect information, and

- to investigate the continuing education of the investigating and prosecuting authorities as well as the judiciary to understand and correctly apply the legislation which may be forthcoming from this investigation.

1.5 Because of the wide scope of the investigation as outlined above, the Commission decided to follow an incremental approach to this investigation. The first stage deals with two questions: the first is whether unauthorised access to computers and the unauthorised modification of computer data and software applications can be dealt with in terms of our criminal law and if not, whether it is desirable that these activities be criminalised. The second is the desirability of introducing procedural provisions aimed at enhancing the investigation and prosecution of these activities.

1.6 During 1998 an issue paper addressing the issues concerning the above-mentioned questions was published. The purpose of the issue paper was to elicit responses in respect of the issues identified and the options raised therein, and to determine whether the Commission has defined the scope of the investigation correctly. Respondents to the issue paper identified three matters to be considered for inclusion in the scope of the investigation. These are:

- the criminalisation of the dissemination of information obtained from unauthorised access to computers;
- the criminalisation of an invasion of a person's privacy through "push marketing", and
- the criminalisation of the disclosure of, and trafficking in, passwords.

These objectives have been included in the scope of the investigation.

CHAPTER 2

2. THE PROBLEM

2.1 Introduction

2.1.1 When one considers the criminalisation of unauthorised accessing of computers and the unauthorised modification of computer data and software applications, there are three questions to be answered. The first is whether the unauthorised accessing of computers and the unauthorised modification of computer data and software applications should attract a criminal sanction. In other words is it justified to sanction these actions with criminal penalties? Secondly, if it is accepted that they should lead to criminal liability, is it necessary to create new offences to criminalise these actions? Thirdly, what provision should be made for the investigation and prosecution of such offences, given the unique nature of electronically stored information?

2.2 Ratio for criminalising unauthorised accessing of computers and unauthorised modification of computer data or software applications

2.2.1 Computers are playing an integral part in the functioning of our society. They are used not only as sophisticated repositories for vast amounts of information but also in operational roles. In these roles computers are relied upon to perform functions upon which human life as well as the economic and industrial functioning of society are dependant. Computers are used, for instance, as instruments in the administering of systems supporting medical treatment, transport control systems, banking and financial systems, communication systems, and national security. The potential danger if computers performing these functions are interfered with is very serious.

2.2.2 As technology advances the risk of computers either becoming the instruments of crime or the targets thereof increases. Consequently computers are becoming particularly vulnerable to crime because of a number of factors: The storage capacity of computers is increasing rapidly. This allows for the centralisation of large amounts of information. More and more computers are connected to open networks such as the Internet. This can allow the transfer of information between systems spanning the globe. Another factor which adds to the vulnerability

of computers is the increased ability to develop software applications that can provide access to systems or cause damage to stored information.

2.2.3 The potential danger which interference with the functioning of a computer holds, coupled with the increased vulnerability of computers to such interference seems to provide sufficient policy grounds for the criminalisation of the actions by means of which information can be obtained from a computer or its functioning be interfered with.

2.2.4 There are a multitude of methods by means of which information can be obtained from a computer or its functioning be interfered with.[1] It would be a very difficult task to describe the elements of each method in order to develop an offence for each. The common denominator among all of these methods is the obtaining of access to a computer without the requisite authority, and this seems to be the basis for the justification for the point of view that unauthorised accessing of a computer should be punishable.

2.2.5 The unauthorised entering of the personal domain of a person is prohibited in respect of physical concepts such as a premises or a building.[2] This personal domain also includes a person's privacy, and therefore an invasion of privacy can lead to criminal liability.[3] It is submitted that in our modern society this personal domain should be extended to include information which is of personal or economic value and which is stored in electronic format.

2.2.6 The potential danger referred to earlier[4] becomes especially relevant when one considers the unauthorised modification of computer data and software applications. This potential danger therefore seems to provide sufficient justification for the criminalisation of such modification of computer data and software applications.

2.2.7 A person's economic interest in his or her tangible property is protected by offences such as theft and malicious injury to property. The demands of our modern society, however,

---

1 Such methods can include the duplication of information on a computer, the removal of information on a computer, the alteration of information stored on a computer, the alteration of the functioning of a computer etc.

2 Section 1 of the Trespass Act, 6 of 1959.

3 The offence of *crimen inuria* prohibits the impairment of a person's *dignitas* which includes his or her privacy.

4 Par. 3.3 *supra*.

necessitate that similar protection be given to a person's intangible interests such as information with personal or economic value stored electronically. This also advocates in favour of the proposition that the unauthorised modification of computer data and software applications should be punishable.

2.3 **Application of current criminal law**

2.3.1 In order to assess whether it is necessary to create new offences to criminalise unauthorised accessing of computers and the unauthorised modification of computer data and software applications, various existing offences will be considered to determine the following two questions:

- can accessing a computer without the express or implied consent of the owner, or the person having control of the computer, be dealt with in terms of our criminal law?
- can the altering of computer data and software applications without the express or implied consent of the owner, or the person having control of the computer, be dealt with in terms of our criminal law ?

2.3.1.1 **Malicious injury to property**

Definition

2.3.1.2 Malicious injury to property is described as the unlawful and intentional damaging of another's property.[5]

Elements of the offence

Damage

2.3.1.3 Damage is caused where property is destroyed, lost, permanently damaged or damaged to such an extent that it reasonably requires repair or that its use is permanently or temporarily interfered with.[6] The damage must furthermore be the consequence of the accused's actions.[7]

---

5 Milton 765; Snyman 544.

6 Milton 771; Snyman 546.

7 Milton 770.

Property

2.3.1.4 The damaged property must be corporeal.[8] The mere invasion of a person's economic sphere is not sufficient.

Culpability

2.3.1.5 The element of culpability is satisfied if there is intent to do the relevant act and to cause the resulting damage.[9]

Application to unauthorised access to computers or unauthorised modification of data and software applications

2.3.1.6 The obtaining of access to a computer, whether authorised or not, does not in itself cause any damage to the computer or to the information stored on it. This seems to exclude any possibility that this offence can be applied to the unauthorised accessing of a computer.

2.3.1.7 A modification of computer data or software applications causing the alteration or destruction of information stored on a computer would have fallen squarely within the description of malicious injury to property. However it must be borne in mind that the property in question must be corporeal.[10] The offence, in its present form, can therefore not be committed in respect of damage caused by means of the modification of computer data and software applications.

2.3.1.8 There is no indication that the courts would consider extending the application of the common law offence of malicious injury to property to incorporeal property such as information stored on a computer. For this to happen a court would have to extend the concept of "property" in the definition of this offence to include intangibles that have economic value to a person.

2.3.1.9 Even if such an extension is to take place it will only relate to the intentional damaging of information stored on a computer. This will still leave open the question whether negligent damage caused by means of the alteration of computer data or software applications should be visited with criminal sanction.

---

8 Milton 771; Snyman 545.

9 Milton 773.

10 See par 2.28 *supra*.

2.3.1.10 Furthermore it is at this stage difficult to speculate how the concept of “damage” in relation to computer data and software applications may be applied. Will any alteration of computer data and software applications which interferes with the use of a computer or computer network be regarded as an injury to property? Or will the court require proof that alteration of computer data or software applications necessitated repair of that specific computer data or software applications or that the use of that specific computer data or software applications has been permanently or temporarily interfered with?

2.3.2 **Housebreaking**

Definition

2.3.2.1 Housebreaking is described as the unlawful breaking into and entering a premises with intent to commit a crime.[11]

Elements of the offence

Breaking

2.3.2.2 The element of “breaking" requires the displacement of an obstruction which forms part of the premises.[12] This does not imply that there has to be any physical damage to the obstruction in question.[13]

Entering

2.3.2.3 Entering takes place if any part of the perpetrator’s person or of any instrument which he or she is using is inserted into the premises.[14] The entry must be unlawful, which means that the perpetrator is not entitled to enter the premises.[15]

Premises

---

11 Milton 792; Snyman 550.

12 Milton 798; Snyman 552.

13 *Ibid*.

14 Milton 801; Snyman 553.

15 Milton 802; Snyman 553.

2.3.2.4 The premises must be a structure which is or may ordinarily be used for human habitation or for storage of property. [16] The structure does not have to be immovable but it is clear that it must be a physical structure.[17]

Culpability

2.3.2.5 The intruder must have the intent to commit some crime other than the entering itself whilst on the premises.[18] The intended offence must not in itself be contained in the breaking and entering.[19] The intent to commit the offence must have been formed when the breaking and entering took place.[20]

Application to unauthorised access to computers or unauthorised modification of data and software applications

2.3.2.6 The difficulties which one encounters in the application of this offence to the unauthorised accessing of computers relate mainly to the fact that the offence was developed to protect the sanctity of the home against intrusions that involve danger to its inhabitants.[21] The elements of the offence are all developed to function in the physical world.

2.3.2.7 The requirement of the presence of a person in a physical structure excludes the possibility that the offence, in its present form, can be applied to the unauthorised accessing of a computer.

2.3.2.8 Even if the gaining of access to a computer can be equated with the element of entering a premises, one is still faced with the problem that the accessing of the computer will have to be connected to the intention to commit another offence. This may not always be possible since the majority of the actions which may follow the accessing of the computer will not lead to criminal liability.

---

16 Milton 803; Snyman 551; **S v Ndhlovu** 1963 (1) SA 926 (T); **S v Ngobeza and Another** 1992 (1) SACR 610 (T).

17 Milton 804.

18 Milton 805; Snyman 554.

19 *Ibid*.

20 Milton 806; Snyman 554.

21 Milton 792; Snyman 554.

2.3.2.9 Just as in the case of the offence of malicious injury to property there is no indication that the courts would consider extending the application of the common law offence of housebreaking to the abstract world of computers and the information stored on them.

2.3.3 **Protection of intellectual property**

2.3.3.1 Copyright in a computer program is protected under the Copyright Act, 1978. Section 11B of this Act describes the nature of copyright in a computer program:

> **11B Nature of copyright in computer programs**
>
> Copyright in a computer program vests the exclusive right to do or authorize the doing of any of the following acts in the Republic:
> (a) Reproducing the computer program in any manner or form;
> (b) publishing the computer program if it was hitherto unpublished;
> (c) performing the computer program in public;
> (d) broadcasting the computer program;
> (e) causing the computer program to be transmitted in a diffusion service, unless such service transmits a lawful broadcast, including the computer program, and is operated by the original broadcaster;
> (f) making an adaptation of the computer program;
> (g) doing, in relation to an adaptation of the computer program, any of the acts specified in relation to the computer program in paragraphs (a) to (e) inclusive;
> (h) letting, or offering or exposing for hire by way of trade, directly or indirectly, a copy of the computer program.

2.3.3.2 Infringement of copyright can lead to criminal liability.[22] Section 27(1) of the Copyright Act, 1978, describes when an infringement of copyright will constitute an offence:

> (1) Any person who at a time when copyright subsists in a work, without the authority of the owner of the copyright-
> (a) makes for sale or hire;
> (b) sells or lets for hire or by way of trade offers or exposes for sale or hire;
> (c) by way of trade exhibits in public;
> (d) imports into the Republic otherwise than for his private or domestic use;
> (e) distributes for purposes of trade; or
> (f) distributes for any other purposes to such an extent that the owner of the copyright is prejudicially affected,

---

22 Section 27 of the Copyright Act, 1978.

> articles which he knows to be infringing copies of the work, shall be guilty of an offence.

2.3.3.3 The maximum penalty that may imposed on a conviction of this offence is a fine or imprisonment for a period of three years in the case of first offenders.[23] In the case of repeat offenders the maximum penalty is a fine or imprisonment for a period of five years. The fine can amount to a maximum of R60 000 for first offenders and R100 000 for repeat offenders.[24]

2.3.3.4 The Copyright Act, 1978, also provides for civil remedies to address infringements of copyright.[25] The remedies provided for include actions for damages, interdicts, actions for the delivery of infringing copies and any other actions which will be at the disposal of a plaintiff in respect of infringements of proprietary rights.[26]

2.3.3.5 A computer program is defined as "a set of instructions fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result".[27] A computer program will be subject to copyright if it is original and if the author is a South African citizen or is domiciled or resident in the Republic or if it is first published or made in the Republic.[28] Copyright initially vests in the author of a work but it may be transferred to third parties.[29]

2.3.3.6 The protection afforded by the Copyright Act, 1978, is very narrowly defined. It is only when one of the actions described in paragraphs (a) to (f) of section 27(1) of this Act is committed in respect of an infringing copy of a computer program that an offence in terms of the Copyright Act, 1978, is committed. This means that criminal liability in terms of section 27(1) of this Act presupposes two elements, namely the existence of an “infringing copy” of a computer program, and the unauthorised distribution of such a copy.

---

23 Section 27(6) of the Copyright Act, 1978.

24 Section 27 (6) of the Copyright Act, 1978 read with section 1 of the Adjustment of Fines Act, 1991.

25 Sections 24 to 26 of the Copyright Act, 1978.

26 Section 24(1) of the Copyright Act, 1978.

27 Section 1 of the Copyright Act, 1978.

28 Section 2 read with sections 3 and 4 of the Copyright Act, 1978.

29 Section 21 of the Copyright Act, 1978.

2.3.3.7 The elements of the offence in section 27(1) of the Copyright Act, 1978, do not in any way relate to the gaining of unauthorised access to a computer. They also do not relate to the alteration or destruction of computer data and software applications. Protection of copyright in a computer program is therefore not wide enough to prevent all forms of abuse of computers or the information stored on computers.

2.3.4 **Trespass**

2.3.4.1 The Trespass Act, 1959, (Act 6 of 1959) creates the offence of entering or being present on fixed property without the requisite permission. Section one of the Trespass Act, 1959, defines the offence as follows:

> (1) Any person who without the permission—
> (a) of the lawful occupier of any land or any building or part of a building; or
> (b) of the owner or person in charge of any land or any building or part of a building that is not lawfully occupied by any person,
> enters or is upon such land or enters or is in such building or part of a building, shall be guilty of an offence unless he has lawful reason to enter or be upon such land or enter or be in such building or part of a building.

2.3.4.2 The penalty prescribed by the Trespass Act, 1959, is a fine not exceeding R2 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment. If the provisions of the Adjustment of Fines Act, 1991 (Act 101 of 1991) are taken into account the maximum fine for trespass is R40 000.

2.3.4.3 The Trespass Act, 1959, clearly prescribes two main elements for the offence of trespass: The entering of, or being present on, land or any building or part of a building on the one hand, and the absence of the requisite permission of the lawful occupier, owner or person in charge of the land or building concerned on the other.

2.3.4.4 The element of entering of, or being present on, land or any building or part of a building requires the physical presence of a person on fixed property. This excludes the possibility that the offence, in its present form, can be applied to the unauthorised accessing of a computer.

2.3.4.5 The elements of the offence of trespass do not include the causing of any damage while being present on the land or building concerned. This offence can therefore in no way be applied to the alteration of computer data or software applications.

2.3.4.6 Since trespass is a statutory offence there is no scope for the courts to extend its application to areas that fall outside the ambit of the Trespass Act, 1959. This would clearly be the case if the provisions of the Trespass Act, 1959, were to be applied to the unauthorised accessing of a computer.

2.4 **Process of criminalisation**

2.4.1 The options to be considered for South Africa therefore seem to be a choice between legislative intervention to create certain offences on the one hand, or to leave the matter to the courts to punish such activities by way of extensions to existing common law offences on the other.

2.4.2 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.

2.4.3 This seems to indicate that the option of introducing new offences by way of legislation should be seriously considered.

2.5 **Procedural aspects**

2.5.1 **Introduction**

2.5.1.1 In the majority of cases where offences are committed through the use of computers there will be some evidence of the offence to be found on a computer. What needs to be considered is whether the procedural aspects of our law are able to provide the tools necessary to detect, investigate and prosecute such offences.

2.5.2 **The Criminal Procedure Act, 51 of 1977**

2.5.2.1 Chapter 2 of the Criminal Procedure Act, 51 of 1977 (hereinafter "the Criminal Procedure Act") provides for a general power of the state to search for and seize certain articles. The articles which are liable to be seized are divided into three categories:

- articles which are concerned with the commission of an offence;
- articles which may afford evidence of the commission of an offence; and
- articles which are intended to be used in the commission of an offence.[30]

2.5.2.2 No limitation is placed on the nature of the article to be seized, as long as it can be included in one of the above-mentioned categories. The purpose of the power to seize articles is to obtain evidence for the institution of a prosecution and to assist the police in their investigation of a case.

2.5.2.3 As a general rule the search for and seizure of the above-mentioned articles must be authorised under a search warrant. A search warrant authorises a police official to search any person identified in the warrant, or to enter and search any premises identified in the warrant.[31]

2.5.2.4 In certain exceptional cases a search may be undertaken without a search warrant. This is when the person concerned consents to the search for and the seizure of the article in question or where the police official, on reasonable grounds, believes that a search warrant will be issued to him or her if he or she applies for such warrant and that the delay in obtaining such warrant would defeat the object of the search.[32]

2.5.2.5 It is clear from the use of words such as "article" and "premises" that the provisions of the Criminal Procedure Act are intended to be applied in respect of physical items. This means that the computer itself may be seized under the provisions of the Criminal Procedure Act. It is doubtful that a warrant can be issued for the search and seizure of specific information contained on a computer.

---

30 Section 20 of the Criminal Procedure Act.

31 Section 21(2) of the Criminal Procedure Act.

32 Section 22 of the Criminal Procedure Act.

2.5.2.6 Just like the offences discussed earlier, the provisions of the Criminal Procedure Act were developed when the idea of a location which is not a physical premises or the seizure of something which is not a tangible object were inconceivable. Although the search of a premises for, and seizure of, a computer itself can be authorised under the Criminal Procedure Act, it is submitted that the same does not apply to the search of a computer and the seizure of information located on that computer.

2.5.2.7 Apart from the application of the Criminal Procedure Act there are other issues in connection with the procedural aspects which must be discussed. These issues are unique to the search for and seizure of information stored on computers and arise from the nature of such information. In the course of this part of the discussion it is accepted for the sake of argument that an investigating officer is authorised to search a computer for certain information.

2.5.3 **Other issues related to the unique nature of electronically stored information**

2.5.3.1 Computers are increasingly linked with other computers to form networks. A computer network can span a building, a province, a country and even the globe. The interconnectivity of computers makes it possible to store information on a computer situated in a remote location which need not even be in the same country as the computer used to store the information.

2.5.3.2 This raises issues related to the validity of a search by means of which information stored in a remote location is located via a network. Normally a search will be authorised in respect of a specific premises where the relevant articles are suspected to be found. In the case of information stored and accessed via a computer network the physical location of the computer containing that information can be very difficult to determine. If the computer on which the information is stored can be located it may be in a location not referred to in the search warrant. The question now arises whether that information can legally be searched for without obtaining another search warrant. If a new search warrant is required, chances are that the information will have been destroyed or altered or moved to another location by the time the warrant is obtained. Such a requirement will furthermore place a near-impossible burden on investigating authorities to obtain accurate information of the exact location of the computer on which the relevant information is stored before applying for a search warrant.

2.5.3.3 The possibility that information may be stored in remote locations also raises issues related to jurisdiction. If the network spans the areas of more than one magisterial district, for

instance, it will be very difficult, if not impossible, to decide who has jurisdiction to issue a search warrant in respect of the relevant information. The issue can be further compounded if the information is distributed over a network in such a way that parts of the relevant in formation are located in one jurisdiction and other parts of it are located in another.

2.5.3.4 If the information searched for is stored via a global network on a computer located outside the Republic, issues of international co-operation will come into play. It may be that the country in which the computer containing the relevant information is located rely strongly on the existence of treaties or conventions as a basis for providing assistance to foreign investigating authorities. It is also possible that the system for the provision of assistance in the foreign country is based on onerous formalities. The delays and difficulties encountered in the area of mutual legal assistance will almost certainly provide an opportunity for the relevant information to be destroyed or altered or moved to another location.

2.5.3.5 It is very probable that when the information searched for is located, it will be found to be protected by security systems such as passwords and encryption. The question arises whether the authority of the investigating officer to do the search is wide enough to entitle him or her to proceed in attempting to get past any obstacle aimed at preventing access to the relevant information. Apart from this there is the practical question of the methods that may be used to overcome such security measures.

2.5.3.6 One of the main functions of a computer is to store information. This may include information of a private nature or information in respect of which an obligation of confidentiality or secrecy exists. The ability to store information in remote locations compounds this issue as the gaining of access to such a computer may infringe on the privacy of other persons not associated with the offence under investigation. Issues of civil liberties, privacy and confidentiality must be considered in respect of the search for and seizure of information stored on a computer. These issues need to be balanced with the need for the effective administration of justice.

2.5.3.7 Since a computer is capable of storing a vast amount of information it is most likely that the information of interest to the investigation officer coexists with other information which is of no interest to him or her. The collateral information found on the computer may be necessary for the day-to-day functioning of a business. This problem is further aggravated if required information is located on a network file server which is crucial to the functioning of a whole

network. In such circumstances it is impossible to remove the computer from the location where it is found.

2.5.4 **Admissibility of evidence**

2.5.4.1 Where an offence is committed by means of a computer or where the computer itself has been the target of illegal activity (such as where unauthorised access has been obtained to a computer) the evidence needed to prove the offence will be found on the computer in question unless steps were taken to destroy that evidence. This means that in order to prove the relevant offence, either the computer itself or a print-out of the information stored on the computer will have to be produced in court.

2.5.4.2 The general rule of the admissibility of evidence is that evidence is admissible if it is relevant to a matter before court.[33] Relevant evidence is evidence tendered to prove or disprove a fact in issue. To this general rule there are a number of exceptions where evidence will be inadmissible in spite of its relevance, such as the rule against hearsay evidence for example.

2.5.4.3 Apart from the general rules as to the admissibility of evidence there are a number of rules prescribing how evidence should be tendered. As a general rule evidence is produced by calling upon a witness to deliver *viva voce* testimony under oath in an open court.[34] Evidence can also be tendered in the form of real evidence or documentary evidence. Real evidence refers to objects produced for inspection by the court so that the court may draw some conclusion in respect of a fact in issue. The object itself is therefore evidence.[35] Documentary evidence is evidence, usually a statement in writing, contained in a document which is intended to prove the truth of its contents.[36] The contents of the document are therefore evidence, as opposed to the document itself.[37]

2.5.4.4 Depending on surrounding circumstances, evidence generated by means of a computer can either be classified as real evidence or documentary evidence. Where a computer print-out

---

33 Schmidt 360; Van der Merwe *et al* 53.

34 Schmidt 245; Van der Merwe *et al* 286.

35 Schmidt 305; Van der Merwe *et al* 269.

36 Van der Merwe *et al* 275.

37 Schmidt 305.

is simply a reflection of a person's knowledge stored in an electronic form it will most likely be classified as documentary evidence. Where the evidence represents the result of the processing of a person's knowledge it will probably be classified as real evidence created by a device.[38] This uncertainty as to the nature of computer-generated evidence raises a number of issues as to how the admissibility of such evidence should be determined. Should the computer print-out be proven to be an original and authentic version of the information it reflects?[39] Should its admissibility be dependant on the proper and reliable functioning of the computer and software applications used to generate the evidence reflected in the print-out?[40] Apart from these issues there are also other, more general, exclusions that may apply, such as that the evidence reflected in the print-out is hearsay for instance.

2.5.4.5 If the issues of admissibility are left out of consideration, one is still faced with the question of how the value to be attached to the evidence should be determined. This will depend very much on the knowledge of the persons producing the evidence - as well as those evaluating it - of computers, their functioning and their capabilities.

2.5.5 **Practical implications of these issues**

2.5.5.1 The following example of what may be found in practice will serve to illustrate the frustrations that may be caused by the issues discussed above. For the sake of this example it is assumed that obtaining unauthorised access to a computer constitutes an offence in terms of a statutory provision. It is further assumed that an investigating officer has received information that a certain computer located at a specific address was used to commit this offence.

2.5.5.2 The investigating officer obtains authority to search for the computer in terms of a search warrant authorised for that purpose. As a result of the search the investigating officer locates the computer in question. However, the owner of the computer objects to the searching of the computer's storage area for any information, as this is not included in the scope of the search

---

38 Schmidt 346.

39 Originality and authenticity are the general requirements for the admissibility of documentary evidence.

40 This would be similar to other evidence produced by means of a device such as a speed measuring apparatus.

warrant. The owner's argument is based on the fact that the information to be searched for is not an "article" and the computer's storage space cannot be described as premises.

2.5.5.3 The only option open to the investigating officer is to seize the computer itself and to remove it from the premises. This decision may, however, be complicated by the fact that the computer equipment belongs to a legitimate business and that it contains information which is crucial to the operation of the business and which is totally unrelated to the information which the investigating officer is searching for.

2.5.5.4 Another problem that may arise in this regard is that the computer on which the relevant information is located may be a file server connected to a huge network which is used for totally lawful purposes, and without which the network cannot function. In such circumstances it is doubtful that the investigating officer will be able to remove the relevant computer from the premises where it is located.

2.5.5.5 The computer which is the target of the search may be shared by a number of users. In such a case the computer will contain collateral information which is not associated with the search. The users of the computer will object to the removal of the computer as this will deprive them of their legitimate use of the computer.

2.5.5.6 If the investigating officer has the authority to search the storage area of the computer, for instance with the consent of the owner, he or she may find that the information in question is encrypted. The owner of the computer, however, objects to the investigation officer's attempts to de-encrypt the information as this is not included in his or her authority to locate that information. Another possibility is that the information is protected by software that will cause the information to be destroyed if it is not accessed in a specific manner. Again the owner of the computer may object to the investigating officer's attempts to circumvent this software as this is not included in his or her authority to locate that information. The owner may also object to such attempts because the investigating officer's actions may alter some information or the functioning of some software on the computer.

2.5.5.7 If it is accepted for the sake of this example that a search of a computer's storage area can be authorised under a search warrant and that the investigating officer has located the computer in question, he or she may find that the computer is linked to other computers via a network. The perpetrator has furthermore made use of this connectivity of the computer in

question to store the relevant information on another computer at a different location which is connected to the same network.

2.5.5.8 The investigating officer is now faced with the problem that the computer which he or she is authorised to search does not contain the relevant information and that he or she is not authorised to search the computer on which that information is contained. By the time a new search warrant is obtained the perpetrator will have moved the information again, or he or she will have altered or destroyed it.

2.5.5.9 Another possibility is that the investigating officer may be unable to determine the location of the computer where the perpetrator has stored the relevant information. This means that the investigating officer is not allowed to search for the relevant information in terms of the search warrant which authorises a search of the computer in question, although it is practically possible to search for that information via the network to which that computer is connected.

2.5.5.10 A third possibility is that the information is stored via the network on a computer located outside the Republic. The investigating officer is now faced with the task of obtaining mutual legal assistance from another country in order to search for the relevant information. By the time all the formalities associated with mutual legal assistance requests have been complied with the perpetrator will have moved the information to another location, or he or she will have altered or destroyed that information.

2.5.5.11 The computer which is the target of the search may contain privileged information which does not relate to the search. The owner of the computer will object to the investigating officer obtaining access to such information in the course of his or her search. It is, however, impossible to locate the relevant information on the storage area of the computer and to sift this from the other information on the computer without accessing all the information on the computer. This may mean that the whole search has to be abandoned.

2.5.5.12 If the investigating officer succeeds in obtaining the relevant information in the course of an authorised search that information must be produced as evidence at the trial of the accused. At this stage the accused may object against the admissibility of the evidence on the basis that the correct procedure for its presentation to the court was not followed or that it constitutes hearsay evidence. If the accused accepts the admissibility of the evidence, he or she may attack the value of the evidence because the information obtained from the computer

may have been altered by the investigating officer, or because the chain of events leading from the collection of the information to its production in court as evidence have not been preserved.

2.5.5.13 All of these pitfalls indicate the near-impossible task of investigating and prosecuting authorities when faced with computer-related offences.

CHAPTER 3

3. INTERNATIONAL EXAMPLES

3.1 Introduction

3.1.1 There are many countries where unauthorised access to computers and unauthorised modification of computer data or software applications have been criminalised. In this chapter we will consider the provisions of a few such countries which will reflect the diverging approaches to the actual definition of these offences.

3.2 Criminalisation of unauthorised access to computers

3.2.1 Australia

3.2.1.1 Part VIA of the Australian Crimes Act 1914 (the "Australian Crimes Act") provides for offences relating to computers. Two of the sections in this Part contain offences concerning access to computer data. The first of these is unlawful access to data in Commonwealth and other computers:

> **- SECT 76B**
> **Unlawful access to data in Commonwealth and other computers**
>
> (1)
> A person who intentionally and without authority obtains access to:
> (a)
> data stored in a Commonwealth computer; or
> (b)
> data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
> is guilty of an offence.
> Penalty: Imprisonment for 6 months.
> (2)
> A person who:
> (a)
> with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
> (b)

intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defence or international relations of Australia;

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence.
Penalty: Imprisonment for 2 years.

(3) A person who:

(a) has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

is guilty of an offence.
Penalty for a contravention of this subsection: Imprisonment for 2 years.

3.2.1.2 The second is that of unlawful access to data in Commonwealth and other computers by means of Commonwealth facility:

- SECT 76D

Unlawful access to data in Commonwealth and other computers by means of Commonwealth facility

(1)

A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence.

Penalty: Imprisonment for 6 months.

(2)

A person who:

(a)

by means of a facility operated or provided by the Commonwealth or by a carrier, with intent to defraud any person and without authority obtains access to data stored in a computer; or

(b)

by means of such a facility, intentionally and without authority obtains access to data stored in a computer, being data that the person knows or ought reasonably to know relates to:

(i)

the security, defence or international relations of Australia;

(ii)

the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii)

the enforcement of a law of the Commonwealth or of a State or Territory;

(iv)

the protection of public safety;

(v)

the personal affairs of any person;

(vi)

trade secrets;

(vii)

records of a financial institution; or

(viii)

commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence.

Penalty: Imprisonment for 2 years.

(3)

A person who:

(a)

by means of a facility operated or provided by the Commonwealth or by a carrier, has intentionally and

without authority obtained access to data stored in a computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

is guilty of an offence.

Penalty for a contravention of this subsection: Imprisonment for 2 years.

3.2.1.3 The two provisions referred to above create essentially similar offences, namely the unauthorised access to computer data which is under government control. The only additional element contained in section 76D is that a facility operated by the government or a telecommunications service provider is used in order to obtain the unauthorised access. This element seems to be superfluous since section 76B does not specify the equipment or the method by means of which the access referred to there is to be obtained. It could therefore include the methods referred to in section 76D. The two sections also contain the same penalties for the corresponding offences. For these reasons we turn our attention to the provisions of section 76B.

3.2.1.4 The focus of the offences of the Australian Crimes Act is the protection of data stored on computers over which the federal government exercises control. This is as opposed to unauthorised access to the relevant computer equipment itself. This recognises the fact that access to computer data can be unauthorised even though the access to the computer by means of which the data in question is accessed, is obtained lawfully.

3.2.1.5 The first offence created in section 76B is that of mere unauthorised access to data stored on a specified computer. For this offence the purpose for which access is obtained or the nature of the specific data is irrelevant.[41]

3.2.1.6 The second offence in section 76B is essentially the same as the first with the additional element that the unauthorised access is obtained with the intent to defraud a person. For the purpose of this offence the nature of the data which is accessed is irrelevant.[42]

---

41 Section 76B(1) of the Australian Crimes Act.

42 Section 76B(2)(a) of the Australian Crimes Act.

3.2.1.7 The third offence in section 76B also comprises the same elements as the first but in this instance the nature of the data to be accessed is qualified. In the case of this offence the purpose for which the unauthorised access is obtained is irrelevant.[43] The types of information that are relevant for this offence can be classified in four categories:

- information relating to the national interest,
- information relating to law enforcement,
- personal information, and
- information of a commercial nature.[44]

3.2.1.8 The additional elements of the second and third offences discussed above add to the seriousness with which they are regarded. These offences are therefore subject to somewhat more severe penalties.[45]

3.2.1.9 Section 76B also contains a fourth offence which is aimed at the situation where a person obtains unauthorised access to data of the nature referred to in paragraph 3.1.5.7 above without initially being aware of the nature of the data concerned. The offence is committed if the person subsequently becomes aware of the nature of the data and then continues to examine it.[46] This offence is aimed at solving problems of proof as to the time when the accused acquired the requisite knowledge of the nature of the data in question.

3.2.2 **United Kingdom**

3.2.2.1 In the United Kingdom the Computer Misuse Act 1990 provides for two offences relating to unauthorised access to computers. The first offence is "unauthorised access to computer material":

> **1 Unauthorised access to computer material**
>
> (1) A person is guilty of an offence if–
>
> (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

---

43 Section 76B(2)(b) of the Australian Crimes Act.

44 Section 76B(2)(b)(i) to (viii) of the Australian Crimes Act.

45 Section 76B(2)(a) and (b) of the Australian Crimes Act.

46 Section 76B(3) of the Australian Crimes Act.

(b) the access he intends to secure is unauthorised; and
(c) he knows at the time when he causes the computer to perform the function that that is the case.

3.2.2.2 This offence is committed when a person causes a computer to perform any function with the intent to secure unauthorised access to a computer program or data held in any computer.[47] The required form of culpability for this offence is intent and the accused must have known the intended access is unauthorised. This is seen as a relatively minor offence and carries a penalty of a fine or imprisonment for a maximum of six months.[48]

3.2.2.3 An important aspect to note about this offence is that the program or data to be accessed need not be located on the computer which performs the function referred to earlier.[49]
3.2.2.4 The purpose for which access is secured is not qualified. As a consequence the offence can be committed even when the purpose for the access is well-meaning.

3.2.2.5 In practice this offence can be committed in a number of ways such as unauthorised use of a person's password, trying to guess a password or installing a program that will obtain a person's password without his or her knowledge. It can even be committed by just switching on a computer which a person is not authorised to use.

3.2.2.6 The second offence is "Unauthorised access with the intent to commit a further offence":

2 Unauthorised access with intent to commit or facilitate commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent–
(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person);
and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

---

47 Section 1 of the Computer Misuse Act 1990.

48 Section 1(3) of the Computer Misuse Act, 1990.

49 Section 1(2) of the Computer Misuse Act 1990.

3.2.2.7 This offence is committed when a person causes a computer to perform any function to secure unauthorised access to computer material with the intent to commit or to facilitate the commission of an offence for which the sentence is fixed by law or for which a term of imprisonment for five years can be imposed.[50] This is seen as a more serious offence and carries a penalty of a fine or imprisonment for a maximum of five years.[51]

3.2.2.8 A factor pointed out in relation to the offences created in the Computer Misuse Act 1990 is that these provisions may not be fully appreciated by the judges, juries and magistrates who have to decide cases relating thereto.[52] If the underlying danger relating to a particular action is not understood it may lead to the questions such as why it is wrong and why is it sufficiently serious to be an offence. If the scope of an offence is perceived to be too wide there will be a reluctance to apply the law with the result that it will become unworkable.

3.2.2.9 A concern which is raised with the offences of the Computer Misuse Act 1990 generally, but which applies especially to the offence of unauthorised access to computer material, is that the Act does not contain categories of offences which distinguish the more serious cases form the less serious ones.[53] This adds to the complexity of the law which may obscure the underlying reasons why computer misuse is criminalised. This may also make it difficult for judicial officers and juries to appreciate the seriousness of computer misuse.

3.2.2.10 It is argued that these factors influenced the jury's decision in the case of **R v Bedworth**.[54] In this case the accused was charged, among other offences, with conspiracy to secure unauthorised access and to cause unauthorised modifications. He did not dispute the evidence against him but raised a defence that he was addicted to computer use, or more specifically computer hacking, and that this had prevented him from forming the necessary intent. In spite of the directions of the presiding judge the jury accepted this defence and acquitted the accused.

---

50 Section 2 of the Computer Misuse Act 1990.

51 Section 2(5) of the Computer Misuse Act 1990.

52 Battcock **The Computer Misuse Act 1990: 5 years on**.

53 *Ibid*.

54 Reported in The Times, 18 March,1993.

3.2.2.11 This adds weight to the view that computer-related offences are not perceived as serious even though the consequences suffered by the victims of those offences are serious.[55] Hackers are perceived as individuals "bucking the system" through some form of eccentric flawed genius.[56]

3.2.3 **Singapore**

3.2.3.1 In Singapore the Computer Misuse Act (Chapter 50A) (below "the Singapore Act") came into being in 1993. This Act corresponds to a large extent with the Computer Misuse Act 1990 of the United Kingdom.

3.2.3.2 The Singapore Act contains an offence of unauthorised access to computer material which is similar to the offence contained in the Computer Misuse Act 1990:[57]

> **3. Unauthorised access to computer material.**
>
> (1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

3.2.3.3 The Singapore Act also contains an offence of unauthorised access to commit or facilitate a further offence:[58]

> **4. Unauthorised access with intent to commit or facilitate commission of further offences.**
>
> (1) Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

---

55 In **R v Bedworth**, *supra*, it was shown that the victims, including an organisation for the research and treatment of cancer, had suffered substantial financial losses.

56 Charlesworth **Legislating against Computer Misuse: The Trials and Tribulations of the Computer Misuse Act 1990**.

57 Section 3 of the Singapore Act.

58 Section 4 of the Singapore Act.

3.2.3.4 This offence applies where the further offence which is intended involves property, fraud, dishonesty or can cause bodily harm.[59]

3.2.3.5 Apart from these offences the Singapore Act contains an offence of unauthorised use or interception of a computer service:[60]

> **6. Unauthorised use or interception of computer service.**
> (1) Subject to subsection (2), any person who knowingly –
> (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;
> (b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; or
> (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),
> shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.

3.2.4 **Canada**

3.2.4.1 In Canada an offence of unauthorised use of a computer was first introduced in the Canadian Criminal Code in 1985.[61]

> **Unauthorized use of computer**
> **342.1** (1) Every one who, fraudulently and without colour of right,
> (*a*) obtains, directly or indirectly, any computer service,
> (*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
> (*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or
> (*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)

---

59 Section 4(2) of the Singapore Act.

60 Section 6 of the Singapore Act.

61 Section 45 of R.S. 1985 c.27 (1st Supp.) which inserted section 342.1 in the Canadian Criminal Code.

> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

3.2.4.2 This section criminalises certain actions relating to the obtaining of a computer service or the interception of a computer function. A "computer service" includes data processing and the storage or retrieval of data.[62] A "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system.[63]

3.2.4.3 In the case of the offences referred to in paragraphs (a) or (b) of section 342.1(1) the purpose for which the computer service was obtained or the computer function intercepted is irrelevant, as long as it was done fraudulently and without colour of right. The use of a computer to commit either of the offences referred to in paragraphs (a) or (b) constitutes a separate offence in terms of paragraph (c).

3.2.4.4 The Canadian approach seems to be focussed on the function or service which a computer renders as opposed to the actual access to the computer or the data or software applications stored on a computer. The offences of section 342.1(1) of the Canadian Criminal Code, especially that of paragraph (c), can therefore be committed by using a computer to which a person has legitimate access.

3.2.4.5 An interesting offence provided for in the Canadian Criminal Code is that of section 342.1(1)(d): using, possessing, or trafficking in computer passwords that would facilitate the commission of one of the other offences of this section. In comments on the options for reform discussed in Issue Paper 14 the introduction of a similar offence in South Africa was also recommended.

3.2.4.6 A further offence relating to computer misuse was introduced in the Canadian Criminal Code in 1997:[64]

Possession of device to obtain computer service

---

62 Section 342.1(2) of the Canadian Criminal Code.

63 *Ibid*.

64 Section 19 of 1997, c18 introduced section 342.2 in the Canadian Criminal Code.

> **342.2** (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,
> (*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
> (*b*) is guilty of an offence punishable on summary conviction.

3.2.4.7 At first glance this provision seems to have a very wide scope. However, the element that the relevant actions must be committed "without lawful justification or excuse" provides a built-in defence in the form of a ground for justification of the accused's actions.

3.2.4.8 This type of offence can be effectively applied to certain software applications which are purposely designed to circumvent security systems or to obtain passwords if such applications can be included in the interpretation of "any instrument or device or any component thereof".[65]

3.2.5 **Germany**

3.2.5.1 The German Criminal Code contains an offence of "data spying":

> Sec. 202a - Data spying
> (1) Anybody who without authority procures himself or another data which are not meant for him and which are specially secured against unauthorised access shall be sentenced to imprisonment not exceeding 3 years or to a fine.
> (2) Data within the meaning of Subsection (1) shall be deemed to be only those which are stored or transmitted electronically, magnetically, or in any other not directly perceptible way.[66]

3.2.5.2 This offence is committed if a person procures data for himself or herself or for another to which he or she or such other person is not entitled and which is specially secured against unauthorised access.[67] The data concerned must be capable of being stored or transmitted

---

65 Examples of such applications are so-called wardialers and trap door programs.

66 Unofficial translation taken from http://www.pcug.co.uk/~drsolly/laws/germany.txt

67 Section 202a(1) of the German StGB.

electronically or magnetically or in any other manner that is not directly perceptible.[68] This offence carries a penalty of a fine or imprisonment for a maximum period of three years.

3.2.5.3 The approach in the German Criminal Code reflects a focus on electronic data instead of the functions of a computer. This facilitates the application of the offence to any method by means of which the data was procured, including the use of a computer to which a person had lawful access. The description of "data" in subarticle (2) is wide enough to refer to data stored on a computer but can, in fact, include much more.

3.2.5.4 It is not clear how the element of procurement of the data concerned is interpreted. In South African terms this element may be interpreted as meaning that the data must be removed from its storage location, or at least that a copy thereof must be made. To merely take account of the data will probably not amount to procurement.

3.2.5.5 The fact that the data concerned was "specially secured against unauthorised access" will in South African circumstances probably be used to indicate that the access of the data was unauthorised. In this sense it would be treated as a fact to prove one of the elements of the offence, rather than one of the substantive elements of the offence.

3.2.5.6 The German Criminal Code also contains a number of offences which protect confidential information against unauthorised disclosure:

Sec. 203 - Violation of private secrets

(1) Anybody who without authority discloses another's secret, especially one relating to the personal sphere of life or an industrial or business secret that has been entrusted to him or has otherwise become known to him in his capacity as
1. physician, dentist, veterinarian, dispensing chemist or member of another healing profession requiring state regulated training for the exercise of the profession or for the bearing of the professional title,
2. professional psychologist with a state recognised scientific final examination,
3. lawyer, patent agent, notary public, defence counsel in proceedings regulated by law, certified public accountant, sworn auditor, tax adviser, authorised tax agent, or an organ, or member of an organ, of a

68 Section 202a(2) of the German StGB

society of certified public accountants, auditors, or tax advisers,

4. marriage, family, educational, or youth counsellor as well as addiction counsellor at a counselling agency that is recognised by public authority or by a corporation, institution, or foundation of public law,

4a. member or agent of a recognised counselling agency under Sec. 218b (2) (No. 1),

5. state recognised social worker or state recognised social educationalist or

6. member of an enterprise of private health, accident, or life, insurance or of an accounting office for private physicians,

shall be sentenced to imprisonment not exceeding one year or to a fine.

(2) Likewise shall be punished anybody who without authority discloses another's secret, especially one relating to the personal sphere of life or an industrial or business secret, that has been entrusted to him or has otherwise become known to him in his capacity as

1. holder of a public office,
2. a person with special obligations with regard to the civil service,
3. a person carrying out tasks or responsibilities under the Personnel Representation Law,
4. member of an investigation committee acting for a Federal, or State, legislative body or of any other committee or council who is not himself a member of the legislative body, or as an assistant of such committee or council, or
5. an officially appointed expert who has been formally obligated for the conscientious compliance with his duties on the basis of legal provisions.

Equivalent to a secret within the meaning of Sentence 1 shall be individual information concerning personal or factual circumstances of another that have been recorded for purposes of public administration; Sentence 1 shall not apply, however, where such individual information is disclosed to other public authorities or other agencies for purposes of public administration and this is not prohibited by law.

(3) Equivalent to the parties mentioned in Subsec. (1) shall be their professionally active assistants as well as persons who are working with them while learning the profession. In addition, after the person charged with the duty of protecting the secret has died, anyone who has obtained knowledge of the secret from the deceased or from his estate shall be deemed equivalent to the parties mentioned in Subsec. (1) and those mentioned in Sentence 1.

(4) Subsections (1 - 3) shall also apply where the offender without authority disclose another's secret after the latter's death.

(5) If the offender discloses the secret for a consideration, or with the intention of enriching himself or another or to injure another, punishment shall be imprisonment not exceeding two years or a fine.[69]

3.2.5.7 These offences prohibit the disclosure and exploitation of confidential industrial or business information or personal information which has become known to a person as a result of a specified relationship.[70] These provisions are wide enough to include information stored on a computer.

3.2.6 **United States of America**

3.2.6.1 The United States has a myriad statutory provisions at federal and state level dealing with various forms of unauthorised access to computer data. At this juncture we will focus our attention of the federal Criminal Code, being a statute of general application.

3.2.6.2 The Computer Fraud and Abuse Act 1986 inserted certain offences relating to misuse of computers in Title 18 of the United States Code, the Criminal Code of the United States:

§1030 Fraud and related activity in connection with computers

(a) Whoever--

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a

---

69 Unofficial translation taken from http://www.pcug.co.uk/~drsolly/laws/germany.txt

70 Sections 203 and 204 of the German StGB.

> card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> (3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;
> (4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;
> (5) ...
> (6) ...
> shall be punished as provided in subsection (c) of this section.

3.2.6.3 This provision creates four offences dealing with unauthorised access to a computer. The main element of the offences created in this provision is the obtaining of unauthorised access to a computer as opposed to the data stored on a computer. This would mean that no offence is committed if a person lawfully obtains access to a computer and then uses that computer to access data which he or she is not authorised to access. Section 1030 of 18 USC addresses this problem by adding the phrase “or exceeds authorized access”.[71]

3.2.6.4 The mere unauthorised accessing of a computer will not be an offence under this provision. In each instance this basic element is coupled with additional elements. These additional elements can be divided into three categories. In the first instance the unauthorised access must lead to the obtaining of certain types of information.[72] In the second instance the nature of the computer to which unauthorised access is obtained is qualified as computers operated by the government.[73] In the last instance the unauthorised access must be coupled firstly with an intent to defraud, and secondly the fact that the intended fraud is in fact furthered

---

71 18 USC 1030(a)(1), (2) and (4).

72 18 USC 1030(a)(1) and (2).

73 18 USC 1030(a)(3).

by the unauthorised access. In this last instance the nature of the computer to which unauthorised access is obtained is also qualified as a "Federal interest computer".[74]

3.2.6.5 Apart from these offences section 1030 of 18 USC also contains an offence of trafficking in passwords:

> (a) Whoever -
>
> (1) - (5) ...
>
> (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
>
> (A) such trafficking affects interstate or foreign commerce; or
>
> (B) such computer is used by or for the Government of the United States;
>
> shall be punished as provided in subsection (c) of this section.

3.2.7 **Council of Europe**

3.2.7.1 The Council of Europe is currently involved in a project to develop a convention on so-called cyber-crime. A draft of this convention was released on 27 April 2000 for discussion and consultation. It is important to take note of the provisions of the Draft Convention on Cyber-Crime (the "draft Convention") as South Africa will have to adopt an approach against the unauthorised access of computers that is compatible with international developments.

3.2.7.2 The draft Convention will place members of the Council of Europe under an obligation to criminalise certain activities. As is normally the case with international instruments of this nature, the draft Convention does not contain exact detail as to the definitions of the offences to be created. This is left to the Parties to the Convention to be done in accordance with the basic legal principles of their respective legal systems.

3.2.7.3 The first offence which the draft Convention will require Parties to create is named "Illegal Access".[75] This refers to the intentional access of a computer system without right. A computer system is defined as "any device or a group of inter-connected devices, which pursuant to a program performs automatic processing of data [or any other function]".[76] This is clearly aimed

---

74 18 USC 1030(a)(4).

75 Article 2 of the draft Convention.

76 Article 1 of the draft Convention.

at the computer itself, as opposed to the data stored on the computer. Parties will be allowed to include two additional elements in their definitions of this offence, namely an infringement of security measures and the intent to obtain computer data.

3.2.7.4 The draft Convention will also contain an obligation to create an offence named "Illegal Interception".[77] This entails the intentional interception of transmissions of computer data without right. Computer data is defined widely enough to include both computer data and software applications stored on a computer.[78]

3.2.7.5 A third offence which will have to be created in terms of the draft Convention relates to "Illegal Devices".[79] This includes the production, sale, procurement, import, distribution, making available or possession of a "device, including a computer program, designed or adapted [specifically] [primarily] [particularly] for the purpose of committing any of the offences" relating to unauthorised access to computers and unauthorised modification of computer data or software applications. The offence to be created under this provision should also cover a "computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed".

3.3 **Criminalisation of unauthorised modification of computer data and software applications**

3.3.1 **Australia**

3.3.1.1 Part VIA of the Australian Crimes Act contains two offences concerning damaging computer data. The first of these is damaging data in Commonwealth and other computers:

> **- SECT 76C**
> **Damaging data in Commonwealth and other computers**
>
> A person who intentionally and without authority or lawful excuse:
>
> (a) destroys, erases or alters data stored in, or inserts data into, a Commonwealth computer;
>
> (b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;

---

77 Article 6 of the draft Convention.

78 Article 1 of the draft Convention.

79 Article 6 of the draft Convention.

(c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

is guilty of an offence.
Penalty: Imprisonment for 10 years.

3.3.1.2 The second is Damaging data in Commonwealth and other computers by means of Commonwealth facility:

- SECT 76E
Damaging data in Commonwealth and other computers by means of Commonwealth facility

A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in, or inserts data into, a computer;

(b) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(c) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a computer;

is guilty of an offence.
Penalty: Imprisonment for 10 years.

3.3.1.3 The two sections referred to above create almost identical offences, namely the damaging of data stored on a computer which is under government control. The only additional element contained in section 76E is that a facility operated by the government or a telecommunications service provider is used in order to obtain the unauthorised access. The two sections also contain the same penalties for the corresponding offences. For these reasons our attention will be focussed on section 76C of the Australian Crimes Act.

3.3.1.4 Apart from the elements of destroying, erasing or altering data, found in other the other examples of this type of offence, the Australian Crimes Act also covers the insertion of data in

a computer.[80] The same offence of the Australian Crimes Act also covers the interfering with the use of a computer and the impeding of access to data stored on a computer. The descriptions of these offences do not require the actions in question to be associated with the destruction or alteration of data, although this is included under the heading of damaging data in computers.

3.3.1.5 The maximum penalty prescribed for these offences is imprisonment for a period of 10 years, which indicates the seriousness with which these offences are regarded.

3.3.2 **United Kingdom**

3.3.2.1 The Computer Misuse Act 1990 provides for an offence of unauthorised modification of computer material:[81]

> **3 Unauthorised modification of computer material**
>
> (1) A person is guilty of an offence if–
>
> (a) he does any act which causes an unauthorised modification of the contents of any computer; and
>
> (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
>
> (2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing–
>
> (a) to impair the operation of any computer;
>
> (b) to prevent or hinder access to any program or data held in any computer; or
>
> (c) to impair the operation of any such program or the reliability of any such data.
>
> (3) The intent need not be directed at-
>
> (a) any particular computer;
>
> (b) any particular program or data or a program or data of any particular kind; or
>
> (c) any particular modification or a modification of any particular kind.
>
> (4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

---

80 Section 76C(a) of the Australian Crimes Act.

81 Section 3 of the Computer Misuse Act 1990.

3.3.2.2 The required form of culpability is intent. The intent must be aimed at causing the modification and thereby to impair the operation of the computer, to prevent access to any program or data or to impair the operation of a program or the reliability of data.[82] There are therefore two elements to the perpetrator's intent, namely to cause the unauthorised modification and for that modification to have certain consequences.

3.3.2.3 The intent described in subsection (3) is a typical example of *dolus indirectus*. It need not be directed at any particular computer, any particular data or software application or any particular type of modification. Consequently this formulation can be applied, for example, to a case where a person develops a virus program which is distributed indiscriminately via e-mail or the Internet.

3.3.2.4 In a commentary on the Computer Misuse Act 1990 it is pointed out that since intent is expressly required as an element of the offence, it does not cover reckless damage or modification.[83] This is as opposed to the corresponding offence of criminal damage of property in English law, which includes reckless acts causing damage.

3.3.2.5 It is also pointed out that the description of the offence in section 3 of the Computer Misuse Act 1990 only refers to "the contents of a computer", in other words data on a computer.[84] This raises a question as to the modification of data on removable storage media such as diskettes. While the data on a storage medium is being accessed by a computer, an argument can be made out that the data is technically "on that computer" even though it is not stored on the computer. However, once the storage medium is removed from the computer the data it contains can no longer be said to be "the contents of a computer".

3.3.3 **Singapore**

3.3.3.1 The Singapore Act provides for an offence of unauthorised modification of computer material:[85]

---

82 Section 3(2) of the Computer Misuse Act 1990.

83 Battcock **The Computer Misuse Act 1990: 5 years on**.

84 *Ibid*.

85 Section 5 of the Singapore Act.

> **5. Unauthorised modification of computer material.**
>
> **(1)** Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 2 years or to both.
>
> **(2)** If any damage caused by an offence under this section exceeds $10,000, a person convicted of the offence shall be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
>
> **(3)** For the purposes of this section, it is immaterial that the act in question is not directed at --
>
> **(a)** any particular program or data;
>
> **(b)** a program or data of any kind; or
>
> **(c)** a program or data held in any particular computer.
>
> **(4)** For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

3.3.3.2 The Singapore Act contains a similar provision to the UK Computer Misuse Act 1990, making it clear that the required intent need not be directed at any particular data or computer.[86] The Singapore Act is therefore also wide enough to apply to a case where a virus program is distributed indiscriminately via e-mail or the Internet.

3.3.3.3 Unlike the corresponding offence of the UK Computer Misuse Act 1990, this offence in the Singapore Act does not expressly require the accused's intent to be aimed at causing any impairment of a computer or any program or data contained on a computer, nor to be aimed at causing any hindrance of access to any program or data. As far as the perpetrator's state of mind is concerned section 5(1) of the Singapore Act only requires that he or she has knowledge that his or her actions will cause an unauthorised modification of the contents of a computer. The consequences of the unauthorised modification are irrelevant to this offence.

3.3.4 **Canada**

3.3.4.1 The Canadian Criminal Code equates the modification of computer data or software applications with damage to property. Damage to property and alteration of computer data or software applications all form part of the offence of "mischief", which is a much wider concept than mere damage to physical property:[87]

---

86 Section 5(3) of the Singapore Act.

87 Section 430 of the Canadian Criminal Code.

PART XI WILFUL AND FORBIDDEN ACTS IN RESPECT OF CERTAIN PROPERTY

430(1) Mischief

430. (1) Every one commits mischief who wilfully

(*a*) destroys or damages property;

(*b*) renders property dangerous, useless, inoperative or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or

(*d*) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

430(1.1) Mischief in relation to data

(1.1) Every one commits mischief who wilfully

(*a*) destroys or alters data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of data; or

(*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

3.3.4.2 The description of the offence in the Canadian Criminal Code does not make reference to the method used to modify or destroy the data in question. Two interesting elements included in this offence are the obstruction of the lawful use of data and the denial of access to data. This may be accomplished without in fact modifying the data in question.[88]

3.3.4.3 Although the offence is headed “mischief” the penalties prescribed indicate that it is regarded as a serious offence. Mischief in relation to data carries a maximum penalty of imprisonment for a period of 10 years.[89] “Data” is defined as “representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system”.[90]

3.3.5 **Germany**

3.3.5.1 The German Criminal Code contains an offence of alteration of data:

---

88 The planting of a so-called logic bomb will be an example of the actions covered by this offence.

89 Section 430(5) of the Canadian Criminal Code.

90 Section 342.1(2) of the Canadian Criminal Code.

Sec. 303a - Alteration of data

(1) Anybody who unlawfully deletes, suppresses, renders useless, or alters data (Sec. 202a (2)) shall be sentenced to imprisonment not exceeding 2 years or to a fine.

(2) The attempt shall be punished.

3.3.5.2 The German Criminal Code also contains and offence of computer sabotage:

Sec. 303b - Computer sabotage

(1) Anybody who interferes with a data processing activity which is of vital importance to another enterprise, another business or a public authority by

1. committing an offence under Sec. 303a (1) or
2. destroying, damaging, rendering useless, removing or altering a data processing system or carrier shall be sentenced to imprisonment not exceeding five years or to a fine.

(2) The attempt shall be punished

3.3.5.3 Data includes data capable of being stored or transmitted electronically or magnetically or in any other manner that is not directly perceptible.[91]

3.3.5.4 The provisions of the German Criminal Code deal with the alteration of data in an abstract manner without associating the alteration of the data with the methods used to accomplish the alteration. This simplifies the definition of the offence an widens its scope.

3.3.6 **United States of America**

3.3.6.1 As was mentioned earlier the Computer Fraud and Abuse Act 1986 inserted certain offences relating to misuse of computers in Title 18 of the United States Code, the Criminal Code of the United States:

§1030 Fraud and related activity in connection with computers

(a) Whoever--

(1) ... ;
(2) ... ;
(3) ... ;
(4) ... ;
(5) intentionally accesses a Federal interest computer without authorization and by means of one or more instances of such conduct alters, damages, or destroys information in any such

---

91 Section 202a(2) of the German StGB

> Federal interest computer, or prevents authorized use of any such computer or information, and thereby--
>
> (A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or
>
> (B) modifies or impairs, or potentially modifies or impairs the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or
>
> (6) ... ;
>
> shall be punished as provided in subsection (c) of this section.

3.3.6.2 This offence contains many more elements than those of Australia, the United Kingdom or Singapore, for example, and therefore has a much narrower scope. Firstly, the alteration of the data must be coupled with the unauthorised access of the computer on which the data in question is stored. Secondly, the data must be stored on a so-called federal interest computer. Lastly the alteration must have caused a loss to another person of at least $1000 within a period of one year, or must have affected the medical care of a person.

3.3.6.3 The fact that the unauthorised alteration of the data in question must be accomplished by means of unauthorised access to a computer severely limits the scope of this offence, especially since the data must be on the computer to which unauthorised access is obtained. This ignores the fact that a person may use a computer to which he or she has legitimate access to alter or destroy data. This provision is probably based on the premise that a person's authority to access a computer ends when he or she uses that computer to commit unlawful acts such as the unauthorised alteration of data. However, this construction adds to the complexity of computer misuse offences. The two concepts of access to computers and alteration of the data on computers are best kept separate.

3.3.6.4 The elements of financial loss or of affecting the medical care of a person may address the issue of the seriousness of the offence under this provision.[92] By proving these elements the prosecution will show the serious nature of the actions in question. However, the inclusion of these elements in the definition of the offence immediately raises the question: What about other instances of alteration of critical data.

---

92 See the discussion concerning the UK Computer Misuse Act 1990 in paragraph 999 to 999 *supra*.

3.3.6.5 If the offence is defined in such a way that it addresses only actions with serious consequences, then one has to ensure that all consequences that are regarded as serious are enumerated in the definition of the offence. It would be very difficult to draft a provision along these lines that includes all instances where alteration of data is of particular concern. This approach is almost certain to result in glaring omissions where specific instances of alteration of data will escape punishment.

3.3.7 **Council of Europe**

3.3.7.1 As was indicated earlier, the Council of Europe has recently published a draft Convention on Cyber-Crime.[93] The draft Convention will include provisions dealing with the unauthorised modification of computer data or software applications.

3.3.7.2 The draft Convention will oblige members of the Council of Europe to establish as criminal offences the intentional damaging, deletion, deterioration, alteration or suppression of computer data.[94] Computer data is defined widely and can include software applications.[95]

3.3.7.3 The draft Convention will also contain an obligation to criminalise the serious hindering of the functioning of a computer system by "inputting, [transmitting,] damaging, deleting, deteriorating, altering or suppressing computer data".[96] The activities referred to in this provision do not entail the modification of data, but can have the same serious effects.

3.4 **Procedural aspects**

3.4.1 **United Kingdom**

3.4.1.1 The Computer Misuse Act 1990 contains only one section dealing with powers of investigation:[97]

14 Search warrants for offences under section 1

---

93 See paragraph 999 *supra*.

94 Article 4 of the draft Convention.

95 Article 1 of the draft Convention.

96 Article 5 of the draft Convention.

97 Section 14 of the Computer Misuse Act 1990.

> (1) Where a circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing–
>
> (a) that an offence under section 1 above has been or is about to be committed in any premises; and
>
> (b) that evidence that such an offence has been or is about to be committed is in those premises;
>
> he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.

3.4.1.2 "Premises" in this provision refers to a physical spaces such as land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.[98] It is not intended to include the storage space of a computer. It seems therefore that although the search for computer in a physical location may be authorised by a search warrant, it is doubtful whether the search for specific information on that computer will be covered by such a warrant.

3.4.1.3 The Police and Criminal Evidence Act 1984 provides for, among other things, general powers of entry, search and seizure which can be executed after arrest:[99]

> **18 Entry and search after arrest**
>
> (1) Subject to the following provisions of this section, a constable may enter and search any premises occupied or controlled by a person who is under arrest for an arrestable offence, if he has reasonable grounds for suspecting that there is on the premises evidence, other than items subject to legal privilege, that relates –
>
> (a) to that offence; or
>
> (b) to some other arrestable offence which is connected with or similar to that offence.
>
> (2) A constable may seize and retain anything for which he may search under subsection (1) above.

3.4.1.4 An investigating officer may furthermore make copies of anything which he or she has the power to seize.[100]

3.4.1.5 These provisions apply to the section 2 offence of the Computer Misuse Act 1990 (unauthorised access with the intent to commit a further crime). However, these powers can

---

98 Section 14(5) of the Computer Misuse Act 1990.

99 Section 18 of the Police and Criminal Evidence Act 1984.

100 Section 21(5) of the Police and Criminal Evidence Act 1984.

only be executed once an offence has been committed. Furthermore, the word "premises" refers to a physical space or location:[101]

> **23 Meaning of "premises" etc**
>
> In this Act–
>
> "premises" includes any place and, in particular includes –
>
> (a) any vehicle, vessel, aircraft or hovercraft;
>
> (b) any offshore installation; and
>
> (c) any tent or movable structure; and
>
> "offshore installation" has the meaning given to it by section 1 of the Mineral Workings (Offshore Installations) Act 1971.

3.4.1.6 This interpretation clearly excludes the storage space of a computer from the meaning of a premises which may be entered and searched.

3.4.1.7 Another area of investigative powers is that of the interception of communication. The Computer Misuse Act 1990 contains no provisions to make this possible. The only legislation which provides for such powers is the Interception of Communications Act 1985:[102]

> **2 Warrants for interception**
>
> (1) Subject to the provisions of this section and section 3 below, the Secretary of State may issue a warrant requiring the person to whom it is addressed to intercept, in the course of their transmission by post or by means of a public telecommunication system, such communications as are described in the warrant; and such a warrant may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such a manner as are described in the warrant.
>
> (2) The Secretary of State shall not issue a warrant under this section unless he considers that the warrant is necessary–
>
> (a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting serious crime; or
>
> (c) for the purpose of safeguarding the economic well-being of the United Kingdom.

3.4.1.8 Against the background of this provision, which is aimed at protecting national security and the prevention or detection of serious offences, it is unlikely that a warrant for the interception of communication will be authorised with a view to the detection and investigation

---

101 Section 23 of the Police and Criminal Evidence Act 1984.

102 Section 2 of the Interception of Communications Act 1985.

of the offences under the Computer Misuse Act 1990.[103] It is pointed out that the interception of communication is a potentially vital tool in the investigation and prosecution of unauthorised access to computers which cannot be effectively applied in respect of the Computer Misuse Act 1990.[104]

3.4.1.9 Apart from the problems relating to the investigation of computer-related offences there are also problems relating to the presence and complexity, not to mention the admissibility, of the evidence that may be involved.[105] The Computer Misuse Act 1990 does not contain any provisions regarding the admissibility of evidence, and this will be determined in accordance with the Police and Criminal Evidence Act 1984. Coupled with the problems relating to the formal admissibility of evidence, there are also problems relating to the reliability of evidence to prove that intrusions occurred and that they were committed by the accused.[106]

3.4.2 **Singapore**

3.4.2.1 In order to facilitate the investigation of the offences of the Singapore Act, a police officer is entitled to have access to and inspect any computer which he or she has reasonable cause to suspect is used in connection with any of the offences created by the Singapore Act:[107]

> **14. Powers of police officer to investigate and require assistance.**
> In connection with the exercise of his powers of investigations under the Criminal Procedure Code, a police officer –
>
> > **(a)** shall be entitled at any time to have access to, and inspect and check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act; and
> > **(b)** may require –
> >
> > > **(i)** the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or

---

103 Battcock **The Computer Misuse Act 1990: 5 years on**.

104 *Ibid*.

105 *Ibid*.

106 *Ibid*.

107 Section 14 of the Singapore Act.

> **(ii)** any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material,
>
> to provide him with such reasonable assistance as he may require for the purposes of paragraph (a).

3.4.2.2 The Singapore Act also provides for the admissibility of evidence in the form of computer output if it is shown that there is no reasonable ground for believing that the output is inaccurate because of improper use of the computer and that no reason exists to doubt or suspect the truth or reliability of the output, and that at all material times the computer was operating properly.[108]

3.4.3 **Council of Europe**

3.4.3.1 The draft Convention of the Council of Europe contains a number of provisions dealing with procedures to assist in the investigation of computer-related crime. These provisions are mainly aimed at the gathering of evidence during the investigation phase of a criminal process.

3.4.3.2 In an article on search and seizure the draft Convention will create an obligation for Parties to the Convention to enact legislation that will empower their investigative authorities to search computer systems and the data stored therein, as well as other media in which computer data may be stored.[109] This provision is specifically aimed at allowing investigators access to the information stored on computer systems in the same way they would have access to physical premises. If South Africa were to incur such an obligation it would mean that provision would have to be made for a search warrant that authorises access to a computer and the information stored on it.

3.4.3.3 The draft Convention provides further that the mechanism by means of which the investigating authorities will be authorised to access a computer system should be wide enough also to authorise access to information stored in another place but which is available to the initial system.[110] In practice this would mean that a search warrant for a computer should also authorise access to remote locations which are accessible from the computer specified in the warrant and the information stored on them. The only caveat is that the remote location should also be subject to the territorial jurisdiction of the country in which the warrant is issued.

---

108 Section 10 of the Singapore Act.

109 Article 14.1 of the draft Convention.

110 Article 14.2 of the draft Convention.

3.4.3.4 Apart from the search powers the draft Convention also provides for the seizure of computer data.[111] The methods that may be used to effect a seizure of information stored on a computer include:

- to seize or similarly secure a computer system or part of it or a medium in which computer data may be stored,
- to make and retain a copy of those computer data,
- to maintain the integrity of the relevant stored computer data, or
- to render inaccessible or remove the computer data in the accessed computer system.

3.4.3.5 The draft Convention takes into account that information stored on computers may be protected by passwords or similar measures. Consequently the draft Convention will oblige Parties to enact legislation empowering the relevant authorities to order a person who has knowledge of the functioning of a computer system, or measures applied to secure the information on the system, to provide all information required for a search and seizure to take place.[112]

3.4.3.6 The draft Convention takes into account that information stored on computers may be protected by passwords or similar measures. Consequently the draft Convention will oblige Parties to enact legislation empowering the relevant authorities to order a person who has knowledge of the functioning of a computer system, or measures applied to secure the information on the system, to provide all information required for a search and seizure to take place.[113]

3.4.3.7 The draft Convention also attempts to address the fact that the information stored on a computer may be of a temporary nature or may be particularly susceptible to modification.[114] This provision will require parties to the Convention to introduce measures enabling its competent authorities to order or otherwise obtain the expeditious preservation of information stored on a computer system.

---

111 Article 14.4 of the draft Convention.

112 Article 14.5 of the draft Convention.

113 Article 14.5 of the draft Convention.

114 Article 16 of the draft Convention.

3.5 **Conclusion**

3.5.1 From this discussion it is clear that there is little uniformity in the descriptions of the relevant offences among the various countries in which the actions of unauthorised access to computers and unauthorised modification of computer data or software applications have been criminalised. It is also clear that it is not sufficient to criminalise only these main offences. One must also introduce related offences which cover all the activities associated with hacking and damaging computer data or software applications.

3.5.2 Another interesting aspect to note is that although many countries have introduced offences to criminalise the relevant activities, not all have introduced special provisions relating to criminal procedure and evidence. This has been pointed out as a major stumbling-block in applying some of these provisions to the investigation and prosecution of the illegal activities.[115] The Council of Europe also seems to realise the importance of this aspect and is going a long way towards addressing it in the draft Convention.

---

115 Battcock **The Computer Misuse Act 1990: 5 years on**.

CHAPTER 4

4. RECOMMENDATIONS

4.1 As indicated in the previous chapter, there are many international examples where unacceptable activities relating to computers are made subject to criminal sanction. It is proposed that the same should apply in South Africa. To achieve this the relevant offences should be established by statute. It is therefore proposed that a "Computer Misuse Act" be developed for this purpose.

4.2 Criminalisation of unauthorised access to computer data and software applications

4.2.1 One of the most widely criminalised activities concerning unauthorised use of computers is unauthorised access to computers. It is proposed that a similar offence be established in South Africa. Careful consideration should, however, be given to the manner in which the elements of such an offence are described.

The criminal action

4.2.2 The methods used to define this criminal activity differ widely from one country to the next. The international examples referred to in the previous chapter reflect a few approaches to the description of the criminal action, each focussing on a different level of access which is prohibited.

4.2.3 One approach is to protect the information on a computer by targeting the functions performed by a computer. In these cases the criminal action entails causing the computer to perform a certain function. This must be coupled with a specific intent to secure access to information stored on a computer.[116]

4.2.4 A more direct approach is to protect the information on the computer itself against unlawful access or procurement. In these cases the criminal action is described with reference

---

116 The UK Computer Misuse Act 1990 and the Singapore Act.

to the information stored on the computer and does not include any reference to the method by means of which access is obtained.[117]

4.2.5 A third approach is to focus on the computer itself. In these cases the criminal action is described as a two-phased action where the first phase is gaining access to a computer. This may be coupled with the commission of other subsequent acts which will be the second phase.[118]

4.2.6 Yet another approach is to define the criminal action with reference to the obtaining of a computer service. The service can include the data processing functions of a computer, in other words the mere use of a computer, as well as data retrieval from a computer.[119]

4.2.7 It is proposed that a wide description of the criminal action be adopted. This description should be aimed at protecting the computer data or software applications stored on a computer system without being limited by references to specific methods by means of which the access is to be obtained. The criminal action of this offence should therefore be described as the obtaining of access to any data and software applications stored on a computer system. In this regard the offence of unlawful access should be comparable to the offence of trespass in terms of physical premises.

4.2.8 The access component of the criminal action should include any manner by means of which a person is enabled to take account of the computer data or use the software applications. Access should therefore be a wide concept and should include all means of taking account of computer data or software applications or of having it output from the computer in which it is held, including on a monitor, printer or storage medium. It should be irrelevant to the description of the criminal action whether the monitor, printer, storage medium or other output device is attached to the computer in which the data or software applications are held or not. In other words it should not only include all instances of copying, moving, or using computer data or software applications but also the mere becoming aware thereof.

Unlawfulness

---

117 The German Criminal Code and the Crimes Act 1914 of Australia.

118 The US Computer Fraud and Abuse Act 1986 and the draft Convention of the Council of Europe.

119 The Canadian Criminal Code.

4.2.9 The element of unlawfulness will be what distinguishes the lawful use of a computer from usage which should be subjected to criminal sanction. This element should be expressed by means of a reference to an absence of authority to obtain the access in question.

4.2.10 The absence of authority is an objectively determinable element. It will be determined with reference to the circumstances of each case. An absence of authority should, in the first instance, entail absence of the permission of the owner or the person lawfully in charge of the computer data or software applications in question. In this regard it must be noted that it is not the absence of permission by the person in charge of the computer by means of which the access is obtained that determines the unlawfulness of that access, but rather the absence of permission by person in charge of the affected computer data or software applications.

4.2.11 The concept of authority entails more than just the permission of the owner or the person lawfully in charge. There are other examples of cases where a person will have authority to access computer data or software applications, such as where the access is authorised in terms of a search warrant.

Culpability

4.2.12 The form of culpability of the unlawful access offence should be intent. The intent should be directed at all the elements of the offence. This implies that the accused must have had the intent to obtain access to the computer data or software applications in question, as well as that he or she must have had knowledge of the unlawfulness thereof.

4.2.13 Knowledge of unlawfulness in these circumstances means that the accused knew that he or she had no authority to access the computer data or software applications in question. The knowledge component of the intent should be interpreted sufficiently widely to include cases of willful blindness. The knowledge component should therefore be interpreted to include circumstances where the accused suspected that he or she might not have authority to access the computer data or software applications in question but nevertheless proceeded to gain access thereto without confirming the presence or absence of the requisite authority. This aspect is, however, not expressly addressed in the proposed Bill as it already forms part of the element of culpability of the proposed offence.

4.2.14 In some of the foreign examples of an unauthorised access offence the element of intent is qualified by a reference to specific motives for the access. These include to cause damage or to make unauthorised modifications to the contents of a computer. In our view this approach is too restrictive. The element of intent should not be linked to a specific purpose or motive for which the unauthorised access is obtained. Again the analogy should be with the offence of trespass in terms of physical premisses.

4.2.15 Based on these remarks it is proposed that the following statutory description be used for the unlawful access offence:

Unauthorised access to or obtaining of applications or data in computer system

... Any person who intentionally and without authority to do so, accesses or obtains any application or data held in a computer system, is guilty of an offence.

4.2.16 It is further proposed that certain concepts be defined in an interpretation clause to assist in the interpretation and application of this offence:

Definitions and interpretation

... (1) In this Act, unless the context indicates otherwise—

"access" in relation to an application or data means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that application or data and includes using the application or data or having it output from the computer system in which it is held in a displayed or printed form, or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not;

"application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function, and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system; and

"computer system" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, one or more of which is capable of—

(*a*) containing data; or

(*b*) performing a logical, arithmetic, or any other function in relation to data;

"data" means any representation of information, knowledge, facts or concepts, capable of being processed in a computer system, and includes such a representation held in any removable storage medium which is for the time being in a computer system.

4.3 **Criminalisation of unauthorised modification of computer data and software applications**

4.3.1 The modification of computer data and software applications is also a common form of computer misuse. It is therefore proposed that a similar offence be established in South Africa.

The criminal action

4.3.2 Similar to the unauthorised access offence it is proposed that the criminal action be widely defined. It should not be limited by any reference to specific methods by means of which the modification is made. The criminal action should therefore include any action which results in a modification of the computer data or software applications concerned.

4.3.3 The criminal action should not contain actual damage resulting from the modification as one of its components. The fact that a modification of computer data or software applications caused damage in any given case should be a factor to take into account upon sentencing.

Unlawfulness

4.3.4 This element should be expressed by means of a reference to an absence of authority to make the modification in question.

4.3.5 The absence of authority should entail absence of permission by the owner or the person lawfully in charge of the computer data or software applications in question. Similar to the

unauthorised access offence, it must be noted that it is the absence of permission by the owner or the person lawfully in charge of the affected computer data or software applications that determines the unlawfulness of the modification.

Culpability

4.3.6 It is recommended that intent should be the required form of culpability for the unlawful modification offence.

4.3.7 The element of intent would naturally include knowledge of the unlawfulness of the modification. In other words the accused must have known that he or she had no authority to cause the modification of the computer data or software applications in question. The knowledge component of the intent for this offence should be interpreted sufficiently widely to make it clear that it includes cases of willful blindness. Consequently the knowledge component should be interpreted to include circumstances where the accused suspected that he or she may not have had authority to cause the modification to the computer data or software applications in question, but nevertheless proceeded with his or her actions, without confirming the presence or absence of the requisite authority. This aspect is, however, not expressly addressed in the proposed Bill as it already forms part of the element of culpability of the proposed offence.

4.3.8 In some foreign examples of an unauthorised modification offence the element of intent is qualified by a reference to specific motives for the modification. These include to impair the operation of a computer or to hinder access to information stored on a computer. In our view this approach is too restrictive. The element of intent should therefore not be linked with a specific purpose or motive for which the unauthorised modification is effected. Instead these motives may form the subjects of separate offences which are not necessarily connected to the unauthorised modification of computer data or software applications.

4.3.9 Based on these remarks it is proposed that the following statutory description be used for the unlawful modification offence:

Unauthorised modification of applications or data in computer system

> **...** (1) Any person who intentionally and without authority to do so, performs an act causing any application or data held in a computer system to be modified, destroyed or erased or otherwise rendered ineffective is guilty of an offence.

4.3.10 It is also proposed that the insertion of computer data or software applications be criminalised on the same basis as the modification of existing computer data or software applications:

> (2) Any person who intentionally and without authority to do so inserts any application or data in a computer system is guilty of an offence.

4.4 Criminalisation of related activities

4.4.1 Apart from the actual unauthorised access and modification offences, there are a few related activities which should also be criminalised. These are the development and trafficking in devices or applications which are primarily used to obtain unauthorised access and the trafficking in passwords. It is also proposed that other activities relating to interfering with the lawful use of a computer be criminalised.

> **Development and trafficking in devices or applications which are primarily used to obtain unauthorised access**
>
> **...** Any person who, without lawful justification, develops, manufactures, produces, imports, exports, procures for use, or makes available, a device or application designed or adapted to make it primarily useful for accessing or for modifying, destroying or erasing or otherwise rendering ineffective an application or data held in a computer system without authority to access, modify, destroy or erase or otherwise render ineffective that application or data, is guilty of an offence.
>
> **Trafficking in computer passwords**
>
> **...** Any person who makes available any password or similar information by means of which an application or data held in a computer system can be accessed without authority to access that application or data, is guilty of an offence.
>
> **Interference with use of computer system**

... Any person who—

(a) prevents or hinders access to any application or data in a computer system;

(b) impairs the effectiveness or reliability of any application or data in a computer system, or

(c) impairs the operation of a computer system,

is guilty of an offence.

4.5 **Procedural porvisions**

4.5.1 It is suggested that certain procedural matters also be addressed in relation to the misuse of computers. These should at least address the issues of search and seizure, admissibility of evidence and jurisdiction.

4.5.2 In this paper the proposed procedural provisions are included in the proposed Computer Misuse Bill. An alternative option is to insert provisions dealing with procedural aspects in relation to the misuse of computers into the Criminal Procedure Act, 1977, where it will fit in with the general provisions on seach and seizure, for instance.

Specific comment on the correct placement of the procedural provisions are invited.

4.5.3 The first of the procedural issues to be addressed is that of search and seizure. It was pointed out above that computers are increasingly linked with other computers to form networks. A computer network can span a building, a province, a country and even the globe. The interconnectivity of computers makes it possible to store information on a computer situated in a remote location which need not even be in the same country as the computer used to store the information.

4.5.3.1 The possibilities for the storing of information via networks demand a different approach toward the search and seizure of such information. For this reason the following provision is proposed:

Search and Seizure

... (1) The State may seize any computer system or take any samples or copies of applications or data–

(a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere;

(b) that may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere; or

(c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

(2) Subject to subsection (5), a computer system referred to in subsection (1) may be seized, or samples or copies of applications or data referred to in that subsection may be taken, only by virtue of a search warrant.

(3) The provisions of section 21 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) shall apply with the necessary changes to the issue and execution of a search warrant referred to in subsection (2).

(4) An investigating official executing a search warrant referred to in subsection (2), may-

(a) at any time search for, have access to, and inspect and check the operation of any computer system, application or data if that official on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant; and

(b) require any person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant.

(5) An investigating official may without a search warrant referred to in subsection (2) seize any computer system or take any samples or copies of applications or data or perform any of the actions referred to in subsection (4)–

(a) if the person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data consents thereto; or

(b) if that official on reasonable grounds believes–

(i) that a search warrant will be issued under subsection (2) if he or she applies for such a warrant; and

(ii) that the delay in obtaining such a warrant would defeat the object of the search.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (4), whether by virtue of a search warrant or in terms of subsection (5) an investigating official shall have due regard for the rights and interests of any person affected thereby to carry on his or her normal activities.

(7) Any person who obstructs, hinders or threatens an investigating official in the performance of his or her duties or the exercise of his or her powers in terms of this section, is guilty of an offence.

4.5.4 The next procedural issue to be considered is that of admissibility of evidence. The offences proposed in this chapter will by nature involve a computer in their commission. It is

therefore extremely likely that either the computer itself or a print-out of the information stored on the computer will have to be produced in court in order to prove the relevant offence.

4.5.5 As was indicated above, there is some uncertainty as to the nature of computer-generated evidence. This raises a number of issues as to how the admissibility of such evidence should be determined. In order to facilitate the prosecution of the relevant offences the following provision is proposed:

Evidence

... (1) Notwithstanding the provisions of any law, information in any medium, including but not confined to data or computer output, shall be admissible as evidence of any fact stated therein in any criminal proceedings in terms of this Act, if it is shown–

(a) that a standard or best procedure, acceptable to the court, has been followed in obtaining the information concerned;

(b) in the event of any departure from such procedure which, in the opinion of the court, is not gravely prejudicial to the accused, such information shall still be admissible as evidence, but the court may then attach correspondingly less weight to such evidence.

(2) For the purposes of deciding on the admissibility and weight of the evidence referred to in subsection (1), the court may draw any reasonable inferences from the circumstances in which the application or data was found, or was originally made or came into being.

4.5.6 The last of the procedural issues to be addressed is jurisdiction. It is very easy to distribute information over a network in such a way that parts of the relevant in formation are located in one jurisdiction and other parts of it are located in another. The fact that computers can be inter-connected even across national borders makes the extension of the courts' ability to apply the offences proposed above a necessity.

4.5.7 This means that a wider concept of the courts' territorial jurisdiction must be applied when approaching the offences to be established in relation to the unauthorised access and modification of computer data or software applications.

4.5.8 It is certainly no understatement to say that the advent of the Internet and e-mail facilities has created a borderless world as far as computer networks are concerned. One has only to recall the effects of recent virus attacks such as those of the "Melissa" and "I love you" viruses

to illustrate this point. Both these viruses spread across the globe in a matter of hours.

4.5.9 To make it clear what our courts' jurisdiction would be in relation to the offences to be created in the proposed Computer Misuse Act, the following provision is proposed:

Territorial jurisdiction

... (1) The provisions of this Act shall apply in relation to any person, whatever his or her nationality or citizenship, outside or within the Republic if—

(a) that person was within the Republic at the time the offence was committed; or

(b) the relevant computer system, application or data was within the Republic at that time.

(2) If an offence under this Act was committed by any person outside the Republic, that person may be dealt with as if the offence was committed within the Republic.

Annexure A: Proposed Computer Misuse Bill

B I L L

To prevent unlawful access to computer material,

ARRANGEMENT OF SECTIONS

BE IT ENACTED by the Parliament o fthe Republic of South Africa as follows:–

CHAPTER 1
INTERPRETATION

Definitions and interpretation

1. In this Act, unless the context indicates otherwise—

(i) "access" in relation to an application or data means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that application or data and includes using the application or data or having it output from the computer system in which it is held in a displayed or printed form, or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not;

(ii) "application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function, and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system;

(iii) "computer system" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, one or more of which is capable of—

(a) containing data; or

(b) performing a logical, arithmetic, or any other function in relation to data;

(iv) "data" means any representation of information, knowledge, facts or concepts, capable of being processed in a computer system, and includes such a representation held in any removable storage medium which is for the time being in a computer system; and

(v) "investigating official" means any law enforcement officer or other official of the State invested by any law with the duty to detect, investigate or uncover the commission of an offence, or to prevent the commission of any offence.

CHAPTER 2
OFFENCES

Unauthorised access to or obtaining of applications or data in computer system

2. Any person who intentionally and without authority to do so, accesses or obtains any application or data held in a computer system, is guilty of an offence.

Unauthorised modification of applications or data in computer system

3. (1) Any person who intentionally and without authority to do so, performs an act causing any application or data held in a computer system to be modified, destroyed or erased or otherwise rendered ineffective is guilty of an offence.

(2) Any person who intentionally and without authority to do so inserts any application or data in a computer system is guilty of an offence.

Development and trafficking in devices or applications primarily used to obtain unauthorised access

4. Any person who, without lawful justification, develops, manufactures, produces, imports, exports, procures for use, or makes available, a device or application designed or adapted to make it primarily useful for accessing or for modifying, destroying or erasing or otherwise rendering ineffective an application or data held in a computer system without authority to access, modify, destroy or erase or otherwise render ineffective that application or data, is guilty of an offence.

Trafficking in computer passwords

5. Any person who makes available any password or similar information by means of which an application or data held in a computer system can be accessed without authority to access that application or data, is guilty of an offence.

Interference with use of computer system

6. Any person who—

(a) prevents or hinders access to any application or data in a computer system;

(b) impairs the effectiveness or reliability of any application or data in a computer system, or

(c) impairs the operation of a computer system,

is guilty of an offence.

CHAPTER 3
PROCEDURAL PROVISIONS

Search and Seizure

7. (1) The State may seize any computer system or take any samples or copies of applications or data–

(a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within the Republic or elsewhere;

(b) that may afford evidence of the commission or suspected commission of an offence, whether within the Republic or elsewhere; or

(c) that is intended to be used or is on reasonable grounds believed to be intended to be

used in the commission of an offence.

(2) Subject to subsection (5), a computer system referred to in subsection (1) may be seized, or samples or copies of applications or data referred to in that subsection may be taken, only by virtue of a search warrant.

(3) The provisions of section 21 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) shall apply with the necessary changes to the issue and execution of a search warrant referred to in subsection (2).

(4) An investigating official executing a search warrant referred to in subsection (2), may-

(a) at any time search for, have access to, and inspect and check the operation of any computer system, application or data if that official on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant; and

(b) require any person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant.

(5) An investigating official may without a search warrant referred to in subsection (2) seize any computer system or take any samples or copies of applications or data or perform any of the actions referred to in subsection (4)–

(a) if the person having charge of, or being otherwise concerned with the operation, custody or care of a computer system, application or data consents thereto; or

(b) if that official on reasonable grounds believes–

(i) that a search warrant will be issued under subsection (2) if he or she applies for such a warrant; and

(ii) that the delay in obtaining such a warrant would defeat the object of the search.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (4), whether by virtue of a search warrant or in terms of subsection (5) an investigating official shall have due regard for the rights and interests of any person affected thereby to carry on his or her normal activities.

(7) Any person who obstructs, hinders or threatens an investigating official in the performance of his or her duties or the exercise of his or her powers in terms of this section, is guilty of an offence.

Evidence

8. (1) Notwithstanding the provisions of any law, information in any medium, including but not confined to data or computer output, shall be admissible as evidence of any fact stated therein in any criminal proceedings in terms of this Act, if it is shown–

(a) that a standard or best procedure, acceptable to the court, has been followed in obtaining the information concerned;

(b) in the event of any departure from such procedure which, in the opinion of the court, is not gravely prejudicial to the accused, such information shall still be admissible as evidence, but the court may then attach correspondingly less weight to such evidence.

(2) For the purposes of deciding on the admissibility and weight of the evidence referred to in subsection (1), the court may draw any reasonable inferences from the circumstances in which the application or data was found, or was originally made or came into being.

Territorial jurisdiction

9. (1) The provisions of this Act shall apply in relation to any person, whatever his or her nationality or citizenship, outside or within the Republic if—

(a) that person was within the Republic at the time the offence was committed; or

(b) the relevant computer system, application or data was within the Republic at that time.

(2) If an offence under this Act was committed by any person outside the Republic, that person may be dealt with as if the offence was committed within the Republic.

CHAPTER 4
GENERAL PROVISIONS

Penalties

10. (1) Any person convicted of an offence contemplated in section 2 or 7(7) shall be liable to a fine, or to imprisonment for a period not exceeding 5 years.

(2) Any person convicted of an offence contemplated in section 3, 4, 5 or 6 shall be liable to a fine, or to imprisonment for a period not exceeding 10 years.

Short title and commencement

11. (1) This Act shall be called the Computer Misuse Act, 200..., and shall come into operation on a date fixed by the President in the Gazette.