

0

SOUTH AFRICAN LAW COMMISSION

ISSUE PAPER 14

Project 108

**COMPUTER-RELATED CRIME:
OPTIONS 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: 26 October 1998

ISBN: 0-621-28710-5

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 -

The Honourable Mr Justice I Mahomed (Chairperson)

The Honourable Mr Justice P J J Olivier (Vice-Chairperson)

The Honourable Madam Justice Y Mokgoro

Adv J J Gauntlett SC

Mr P Mojabelo

Prof R T Nhlapo

Ms Z Seedat

The Secretary is Mr W Henegan. The Commission's offices are on the 12th floor, Sanlam Centre, cnr 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 : psmit@salawcom.org.za

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

PREFACE

This issue paper (which reflects information gathered up to the end of July 1998), 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 contained herein should not, at this stage, be regarded as the Commission's final views. The 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 focussed submissions before the Commission.

The Commission will assume that respondents agree to the Commission's 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 26 October 1998 at the address appearing on the previous page. The researcher will endeavour to assist you with particular difficulties you may have. Comment already forwarded to the Commission should not be repeated; in such event respondents should merely indicate that they abide by their previous comment, if this is the position.

The researcher allocated to this project, who may be contacted for further information, is Pieter Smit. The project leader responsible for this project is Prof D P van der Merwe.



CONTENTS

| | Page |
|----------------------|-------------|
| INTRODUCTION | (ii) |
| PREFACE | (iii) |
| CONTENTS | (iv) |
| SOURCES AND CITATION | (v) |
| TABLE OF CASES | (vi) |
| SELECT LEGISLATION | (vi) |

CHAPTER 1

| | |
|------------------------------------|----------|
| Introduction and background | 1 |
|------------------------------------|----------|

CHAPTER 2

| | |
|--------------------|----------|
| The problem | 3 |
|--------------------|----------|

| | |
|---|---|
| Malicious injury to property and unauthorised access to computers | 3 |
| Damage | 3 |
| Property | 3 |
| Culpability | 4 |

| | |
|---------------|---|
| Housebreaking | 4 |
| Breaking | 4 |
| Entering | 5 |
| Premises | 5 |
| Culpability | 5 |

| | |
|---|---|
| Malicious injury to property and unauthorised modification of computer data and software applications | 6 |
|---|---|

| | |
|-------------------------------------|---|
| Protection of intellectual property | 6 |
|-------------------------------------|---|

| | |
|--|---|
| Procedural aspects | 8 |
| The Criminal Procedure Act, 51 of 1977 | 8 |

CHAPTER 3



| | |
|---|-----------|
| Identifying issues | 10 |
| Criminalisation of unauthorised accessing of computers and unauthorised modification of computer data and software applications | 10 |
| Application of the criminal law | 11 |
| Application of the Criminal Procedure Act | 12 |
| Issues arising from the unique nature of electronically stored information | 12 |
| Admissibility of evidence | 15 |
| Practical implications of these issues | 16 |
| | |
| CHAPTER 4 | |
| Options for reform | 20 |
| Criminalisation of unauthorised access to computers | 20 |
| United Kingdom | 20 |
| Singapore | 25 |
| Germany | 27 |
| Unauthorised modification of computer data and software applications | 27 |
| United Kingdom | 27 |
| Singapore | 28 |
| Germany | 29 |
| Options to consider | 29 |
| | |
| CHAPTER 5 | |
| The way forward | 32 |

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
http://www.strath.ac.uk/Departments/Law/student/PERSONAL/R_BATTCKOCK/crime1.html accessed on 10 December 1997.

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

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)

SELECT LEGISLATION

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)

Singapore

- 1993 Computer Misuse Act 1993

United Kingdom

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

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 project committee realises that the scope of an investigation into computer related crime is very wide. For this reason the committee set six objectives which it aims to achieve during the course of the investigation. These are:

1.4.1 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,

1.4.2 to investigate the possibility of providing for the procedural aspects associated with the investigation and prosecution of the above-mentioned offences,

1.4.3 to investigate the use of computers to commit offences such as theft and fraud,

1.4.4 to investigate offences committed by means of the Internet,

1.4.5 to investigate matters relating to encryption in order to protect information, and

1.4.6 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 the this investigation.

1.5 Because of the wide scope of the investigation as outlined above the committee decided to follow an incremental approach to this investigation. The first stage, which will be the topic of this issue paper, will explore 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 The purpose of this Issue Paper is twofold: on the one hand, to elicit responses in respect of the issues identified and the options raised herein, and on the other hand, to determine whether the Commission is aware of all the issues pertaining to unauthorised access to computers and the unauthorised modification of computer data and software applications and the related procedural matters and whether there are other options of reform in respect of any of these issues which should be considered. Respondents are therefore invited, not only to comment on the issues and options discussed in this paper, but also to indicate whether they agree with the scope of the investigation and the according of priorities to the various objectives as set out above and to raise other issues and option which may be relevant to the subject matter thereof.

CHAPTER 2

2 THE PROBLEM

2.1 In order to assess the extent of the problems currently experienced various existing offences will be considered to determine the following question: 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? The same will also be done in respect of the unauthorised altering of computer data and software applications.

Malicious injury to property and unauthorised access to computers

2.2 Malicious injury to property is described as the unlawful and intentional damaging of another's property.¹

Damage

2.3 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.² The damage must furthermore be the consequence of the accused's actions.³

Property

2.4 The damaged property must be corporeal.⁴ The mere invasion of a person's economic sphere is not sufficient.

Culpability

2.5 The element of culpability is satisfied if there is intent to do the relevant act and to cause the resulting damage.⁵

1 Milton 765; Snyman 544.

2 Milton 771; Snyman 546.

3 Milton 770.

4 Milton 771; Snyman 545.

5 Milton 773.

2.6 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.

2.7 The alteration or destruction of information stored on a computer, which may follow the unauthorised accessing of a computer, would have fallen squarely within the description of malicious injury to property were it not for the requirement that the damaged property has to be corporeal. There is no indication that the courts would consider extending the common law to apply to incorporeal property such as information stored on a computer. Even if such an extension is to take place it will only relate to the intentional damaging of information stored on a computer; something which can be done after obtaining authorised access to a computer.

Housebreaking

2.8 Housebreaking is described as the unlawful breaking into and entering a premises with intent to commit a crime.⁶

Breaking

2.9 The element of "breaking" requires the displacement of an obstruction which forms part of the premises.⁷ This does not imply that there has to be any physical damage to the obstruction in question.⁸

Entering

2.10 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.⁹ The entry must be unlawful which means that the perpetrator is not entitled to enter the premises.¹⁰

6 Milton 792; Snyman 550.

7 Milton 798; Snyman 552.

8 *Ibid.*

9 Milton 801; Snyman 553.

10 Milton 802; Snyman 553.

Premises

2.11 The premises must be a structure which is or may ordinarily be used for human habitation or for storage of property.¹¹ The structure does not have to be immovable but it is clear that it must be a physical structure.¹²

Culpability

2.12 The intruder must have the intent to commit some crime other than the entering itself whilst on the premises.¹³ The intended offence must not in itself be contained in the breaking and entering.¹⁴ The intent to commit the offence must have been formed when the breaking and entering took place.¹⁵

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.¹⁶ The elements of the offence are all developed to function in the physical world. 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. Another problem is that the accessing of the computer must be connected to the intention to commit another offence. As can be seen from the discussion above this may not always be possible because the majority of the actions which may follow the accessing of the computer will not lead to criminal liability.

2.13 It is extremely doubtful that our courts would be willing to extend the application of the elements of housebreaking to the abstract world of computers and the information stored on them.

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

12 Milton 804.

13 Milton 805; Snyman 554.

14 *Ibid.*

15 Milton 806; Snyman 554.

16 Milton 792; Snyman 554.

Malicious injury to property and unauthorised modification of computer data and software applications

2.14 The property in question must be corporeal.¹⁷ The offence can therefore not be committed in respect of damage caused by means of the modification of computer data and software applications.

Protection of intellectual property

2.15 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.

2.16 Infringement of copyright can lead to criminal liability.¹⁸ Section 27(1) of the Copyright Act, 1978, describes when an infringement of copyright will constitute an offence:

17 See par 2.28 *supra*.

18 Section 27 of the Copyright Act, 1978.

(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,

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

2.17 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.¹⁹ 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.²⁰

2.18 The Copyright Act, 1978, also provides for civil remedies to address infringements of copyright.²¹ 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.²²

2.19 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".²³ 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.²⁴ Copyright initially vests in the author of a work but it may be transferred to third parties.²⁵

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

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

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

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

23 Section 1 of the Copyright Act, 1978.

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

25 Section 21 of the Copyright Act, 1978.

2.20 The protection afforded by the Copyright Act, 1978, is very narrowly defined and exists only if the conditions discussed in the preceding paragraphs are met. 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.

Procedural aspects

2.21 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.

The Criminal Procedure Act, 51 of 1977

2.22 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:

2.22.1 articles which are concerned with the commission of an offence;

2.22.2 articles which may afford evidence of the commission of an offence; and

2.22.3 articles which are intended to be used in the commission of an offence.²⁶

2.23 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.

26 Section 20 of the Criminal Procedure Act.

2.24 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.²⁷

2.25 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.²⁸

2.26 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.

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

28 Section 22 of the Criminal Procedure Act.

CHAPTER 3

3 IDENTIFYING ISSUES

Criminalisation of unauthorised accessing of computers and unauthorised modification of computer data and software applications

3.1 The first issue which needs to be considered is whether the unauthorised accessing of computers and the unauthorised modification of computer data and software applications should attract a criminal sanction. This issue relates on the one hand to the question whether it is justified to sanction these actions with criminal penalties. On the other hand it relates to the question whether it is necessary to create new offences to criminalise these actions, if it is accepted that they should lead to criminal liability.

3.2 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 for instance where they administer banking and financial systems, transport control systems, communication systems and a variety of other complex operations.

3.3 The potential danger if computers performing these functions are interfered with is very serious. This potential danger alone seems to provide a policy ground for the criminalisation of the actions by means of which information can be obtained from a computer or its functioning interfered with. It should, however, be clear that there are a multitude of methods by means of which information can be obtained from a computer or its functioning interfered with.²⁹ 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.

29 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.

3.4 The unauthorised entering of the personal domain of a person is prohibited in respect of physical concepts such as a premises or a building.³⁰ This personal domain also includes a person's privacy and therefore an invasion of privacy can lead to criminal liability.³¹ 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.

3.5 The potential danger referred to earlier³² become 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.

3.6 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, necessitates 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.

Application of the criminal law

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

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

32 Par. 3.3 *supra*.

3.7 The common law offences discussed in Chapter 2 were developed in a world where computers and the abstract concepts such as information with personal or economic value being stored on computers were unknown. All of these offences were developed to apply to physical objects and can therefore not be applied to activities done in respect of the above-mentioned abstract concepts. It is clear that none of these offences can, in their present form, provide a criminal sanction to the unauthorised accessing of computers. There is furthermore no indication that the courts would be willing to extend the application of any of these offences to apply to computers and the information stored on them.

3.8 The protection afforded by the Copyright Act, 1978, only relates to "computer programmes" as defined in the Act. It does therefore not include all information that can be stored on a computer such as computer databases for example. Before copyright can be infringed it must be proven to exist as provided for in sections 2 to 4 of the Copyright Act, 1978. In the majority of cases the affected computer data or software applications will either not be eligible for copyright (because it is not an original work) or the person whose interest is affected will not be the author.

3.9 For criminal liability to result from a copyright infringement the actions by means of which the right is infringed must fall within the scope of section 27 of the Copyright Act, 1978. This does not include the alteration or destruction of the work in which the copyright subsists, for example.

Application of the Criminal Procedure Act

3.10 Just like the common law 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.

Issues arising from the unique nature of electronically stored information

3.11 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.

3.12 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.

3.13 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.

3.14 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 information are located in one jurisdiction and other parts of it are located in another.

3.15 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.

3.16 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.

3.17 One of the main functions of a computer is to store information. This may include information of 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.

3.18 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 coexist 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.

Admissibility of evidence

3.19 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.

3.20 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.

3.21 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 is therefore evidence as opposed to the document itself.³⁷

3.22 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 is

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.

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, exclusion that may apply such as that the evidence reflected in the print-out is hearsay for instance.

3.23 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.

Practical implications of these issues

3.24 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.

3.25 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 premisses.

3.26 The only option open to the investigating officer is to seize the computer itself and to remove it from the premisses. 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.

3.27 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 premisses where it is located.

3.28 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.

3.29 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.

3.30 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.

3.31 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.

3.32 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.

3.33 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.

3.34 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.

3.35 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.

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

CHAPTER 4

4 OPTIONS FOR REFORM

4.1 Against the background of the issues identified in Chapter 3 the options for reform will now be discussed.

Criminalisation of unauthorised access to computers

United Kingdom

4.2 In the United Kingdom the Computer Misuse Act 1990 came into being as a result of investigations into computer crime by the Scottish Law Commission and the Law Commission for England and Wales.

4.3 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;
- (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.

4.4 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.⁴¹ The required form of culpability for this offence is intent and the accused must have known the intended access is unauthorised. The important aspect to note about this offence is that the

41 Section 1 of the Computer Misuse Act 1990.

program or data to be accessed need not be located on the computer which performs the function referred to earlier.⁴²

4.5 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.

4.6 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.⁴³

4.7 In a commentary on the Computer Misuse Act 1990 it is reported that there were nine known prosecutions for the above-mentioned offences until June 1995. All but one of these involved "internal" incidents where the unauthorised access was obtained by employees or ex-employees.⁴⁴

4.8 The Computer Misuse Act 1990 contains only one section dealing with powers of investigation:⁴⁵

14 Search warrants for offences under section 1

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

43 Section 2 of the Computer Misuse Act 1990.

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

45 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.

4.9 "Premises" in this provision refers to a physical spaces such as land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.⁴⁶ 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.

4.10 The Police and Criminal Evidence Act 1984 provides for, among others, general powers of entry, search and seizure which can be executed after arrest.⁴⁷

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.

4.11 An investigating officer may furthermore make copies of anything which he or she has the power to seize.⁴⁸

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

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

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

4.12 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 only be executed once an offence has been committed. Furthermore, the word "premises" refers to a physical space or location.⁴⁹

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.

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

4.13 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 1985:⁵⁰

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

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

50 Section 2 of the Interception of Communications Act 1985.

(c) for the purpose of safeguarding the economic well-being of the United Kingdom.

4.14 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 of the offences under the Computer Misuse Act 1990.⁵¹ 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 1990.⁵²

4.15 Apart from the problems relating to the investigation of computer related offences there are also problems relating to the amounts and complexity, not to mention the admissibility, of the evidence that may be involved.⁵³ 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 related 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.⁵⁴

4.16 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.⁵⁵ If the underlying danger relating to a particular action is not understood it may lead to the question of 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.

Singapore

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

52 *Ibid.*

53 *Ibid.*

54 *Ibid.*

55 *Ibid.*

4.17 In Singapore the Computer Misuse Act (Chapter 50A) (hereafter "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.

4.18 The Singapore Act contains an offence of unauthorised access to computer material which is similar to the offence contained in the Computer Misuse Act 1990:⁵⁶

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.

4.19 The Singapore Act also contains an offence of unauthorised access to commit or facilitate a further offence:⁵⁷

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.

4.20 This offence applies where the further offence which is intended involves property, fraud, dishonesty or can cause bodily harm.⁵⁸

56 Section 3 of the Singapore Act.

57 Section 4 of the Singapore Act.

58 Section 4(2) of the Singapore Act.

4.21 Apart from these offences the Singapore Act contains an offence of unauthorised use or interception of a computer service:⁵⁹

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.

4.22 In order to facilitate the investigation of these offences 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.⁶⁰

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

(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).

4.23 The 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

59 Section 6 of the Singapore Act.

60 Section 14 of the Singapore Act.

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.⁶¹

Germany

4.24 The German Criminal Code contains an offence of "data spying". 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.⁶² The data referred to here must be capable of being stored or transmitted electronically or magnetically or in any other manner that is not directly perceptible.⁶³

4.25 The German Criminal Code also contains a number of offences which protect confidential information against unauthorised disclosure. 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.⁶⁴ These provisions are wide enough to include information stored on a computer.

Unauthorised modification of computer data and software applications

United Kingdom

4.26 The Computer Misuse Act 1990 provides for an offence of unauthorised modification of computer material:⁶⁵

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

61 Section 10 of the Singapore Act.

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

63 Section 202a(2) of the German StGB.

64 Sections 203 and 204 of the German StGB.

65 Section 3 of the Computer Misuse Act 1990.

(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.

4.27 The required form of culpability is intent and 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. In a commentary on the Computer Misuse Act 1990 it is reported that there were ten known prosecutions for the above-mentioned offences until June 1995.⁶⁶

4.28 The comments made earlier in respect of the offences relating to the unauthorised access to computers also apply in respect of the offence of unauthorised modification of computer material. The problems in respect of the application of this offence relate mainly to the powers of investigation and the admissibility of evidence.

Singapore

4.29 The Singapore Act provides for an offence of unauthorised modification of computer material:⁶⁷

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.

4.30 This offence does not 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.⁶⁸

66 Battcock **Computer Misuse Act 1990: 5 years on.**

67 Section 5 of the Singapore Act.

Germany

4.31 The German Criminal Code contains an offence of alteration of data. This offence is committed if a person unlawfully deletes, suppresses, or alters data or renders such data useless.⁶⁹ Data includes data capable of being stored or transmitted electronically or magnetically or in any other manner that is not directly perceptible.⁷⁰

Options to consider

4.32 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.

4.33 It has already been suggested earlier that there is no indication that an extension of the common law offences is likely. This possibility relates to 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.

4.34 This seems to indicate that the option of introducing new offences by way of legislation should be seriously considered. In this respect there seems to be a choice between two approaches: The approach followed in the legislation of the United Kingdom and Singapore is to protect the relevant information on a computer by targeting the function performed by a computer. In each of the various offences the *actus reus* entails to cause the computer to perform

68 Section 5(3) of the Singapore Act.

69 Section 303a of the German StGB.

70 Section 202a(2) of the German StGB

a certain function. In Germany a more direct approach is followed by protecting the information on the computer itself against unlawful procurement or alteration.

4.35 In respect of the offences relating to unauthorised access it needs to be considered whether unauthorised access and unauthorised access with the intent to commit a further offence should be created as two separate offences.

4.36 The scope of such offences should also be considered. It should not be so wide as to include trivial cases of misuse which were not intended to be included in the scope of the legislation.

4.37 In respect of the unauthorised modification of computer material it should be considered whether this offence should be the equivalent of the common law offence of malicious injury to property or whether it should also include negligent modifications to computer material or modifications made for a purpose other than to impair the operation of the computer or to compromise the data stored on a computer.

4.38 As a result of the ability to use computers to commit offences across international borders the issue of extradition should be considered. An "extraditable offence" is:⁷¹

any offence which in terms of the law of the Republic and of the foreign State concerned is punishable with a sentence of imprisonment or other form of deprivation of liberty for a period of six months or more, but excluding any offence under military law which is not also an offence under the ordinary criminal law of the Republic and of such foreign State;

71 Section 1 of the Extradition Act 67 of 1962.

Any offences in respect of unauthorised access to computers and unauthorised modification of computer material should be formulated in such terms that the provisions of the Extradition Act 67 of 1962 will apply to them.

4.39 If the example of the Singapore Act is followed there is also the option of creating procedures for the detection, investigation and prosecution of these offences. This includes the introduction of search and seizure powers which are developed to be applied in relation to abstract concepts such as information stored on computers, and the admissibility as evidence of information gathered in this manner. A further option to be considered in this regard is that of the interception of computer communication.

CHAPTER 5

5 THE WAY FORWARD

5.1 It is suggested that the issues and options relating to the unauthorised access to computers and the unauthorised modification of computer data and software applications be debated thoroughly before any direction is embarked upon. This debate should also include the options for procedural provisions in order to facilitate the detection, investigation and prosecution of unauthorised access to computers and the unauthorised modification of computer data and software applications.

5.2 Based on the outcome of such discussions legislation in respect of investigation and prosecution of unauthorised access to computers and the unauthorised modification of computer data and software applications as well as related procedural aspects may be proposed. The comments of all parties who feel that they have an interest in this topic or may be affected by the type of measures discussed in this paper are therefore of vital importance to the Commission.

5.2. To facilitate a focussed debate, respondents are requested to formulate crisp submissions with the following in mind:

5.2.1 do respondents agree with the scope of the investigation and the according of priorities to the various objectives as set out in paragraphs 1.4 and 1.5 of Chapter One of this Issue Paper;

5.2.2 is there a need for legislative intervention to create the offences of unauthorised access to computers and the unauthorised modification of computer data and software applications;

5.2.3 is there a need for the introduction of procedural provisions developed specifically to be applied in relation to computer related offences;

5.2.4 is it agreed that the principal issues are those set out in this paper,

5.2.5 are there any other issues pertaining to the unauthorised access to computers, the unauthorised modification of computer data and software applications and the related procedural matters which were not discussed in this paper, and

5.2.6 what, specifically, is proposed in relation to those issues (or any further issues) as an effective basis for reformatory legislation?

5.3 All respondents are invited to indicate their preferences in respect of the options examined and to raise other issues and options of which the Commission may be unaware and which they feel should be explored.