Name: Tafadzwa Sithole

Student number: STHTAF001

Course: LLM Dissertation

Title: E- Crime under Section 86 of the Electronic Communications Act

Supervisor: Professor J Hofman

Word Count: 18 415 Words

Contact details:

Cell phone: 084 832 66 56

Telephone: (011) 291 5000

Email: misstafadzwa@webmail.co.za

This paper was done in partial fulfillment of the requirements of the LLM degree.

Chapter 7 Conclusion

E- Crime under Section 86 of the Electronic Communications Act

Chapter 1

Introduction

The modest objective of this research paper is to provide a general overview of the phenomenon commonly known as e-crime or computer crime. More specifically, the discussion will center on section 86 of the Electronic Communications Act (ECT Act).[1] The application of the criminal law provisions found in section 86 will be examined. Attempts will also be made to interpret the section. As with almost any new piece of legislation, interpretation problems may arise. Where this is the case, possible recommendations will be made.

Lastly, the paper will focus on some the crimes that are not found in the Electronic Communications Act. The main task in this part of the paper is to determine whether the common law is sufficient to deal with these new offences. Conducts known as phishing, advance fee fraud, identity theft and cyber stalking will be discussed.

[1] Electronic Communications Act No. 25 of 2002

There is no agreed definition of computer crime.[2] A distinction is made between cyber crime and computer crime. Cyber crime[3] is defined as any crime that involves computers and networks including crimes that do not rely heavily on computers. Computer crimes on the other hand, are a special type of cyber crime. The term mainly refers to a limited set of crimes that are specifically defined in laws such as the United States' Computer Fraud and Abuse Act.[4] These crimes include the theft of computer services, unauthorized access to protected computers, software piracy and the alteration or theft of electronically stored information. The crime also includes the extortion committed with the assistance of computers, obtaining unauthorized access to records from banks, credit card issuers, or customer reporting agencies, traffic in stolen passwords and transmission of destructive viruses or commands.[5]

1.1 History of South African ECT Legislation

Prior to the enactment of the Electronic Communications Act, the South African Law Commission pondered on whether legislation such as the Electronic Communications Act was necessary. One of the questions that the Law Commission asked was whether unauthorized access to computers and unauthorized modification of computer data and software could be dealt with in terms of our criminal law and if not, whether it was desirable to criminalize these activities. The project team considered whether the

[2] Buys R (ed.) *Cyberlaw@SA: The Law of the Internet in South Africa* (2004) 320 See also Van der Merwe 'Computers' Law of South Africa vol. 5, Part 3 (1998)
[3] Cyber crimes are generally made possible by the combination of computers with telecommunications abilities
[4] 18 USC 1030
[5] Buys (n 2) 320

common law crimes such as malicious injury to property, housebreaking and trespass could be applied to internet related crime.[6]

The project team was tasked to investigate the criminalization of unauthorized access to computers as well as unauthorized modification of computer data and software applications which includes the planting of a virus for example. The project team was also tasked to investigate the use of computers to commit offences such as fraud and theft. One of the other objectives that the project team was to investigate was the possibility of providing for the procedural aspects associated with the investigation and prosecution of offences committed by means of the internet.[7]

The outcome of the Law Commission's investigations was that electronic crime legislation was necessary in South Africa. The project team proposed that legislation should criminalize activities such as the unauthorized modification of computer data and software, fraud and theft committed by means of a computer. The project leader, Professor Van der Merwe, pointed out that if it were not for the problem of legality the courts would have been able to extend the definition of present common-law crimes to encompass "computer-spawned" criminal activity.[8] If the courts were able to extend the common law crimes to computer-related crimes, "hacking" into someone else's computer over a network might have been seen as a form of electronic trespassing, and planting a

[6] South African Law Commission *Computer Related Crime: Preliminary Proposals For Reform In Respect of Unauthorized Access to Computers, Unauthorized Modification of Computer Data and Software Applications and Related Procedural Aspects* (Project 108) Discussion Paper 99 (2001) 5 - 11
[7] South African Law Commission (n 6) 1
[8] Buys (n 2) 320

virus program to carry on unpredictable operations in some else's computer might have been seen as malicious injury to property.[9]

1.2 Current South African Legislation

The Electronic Communication Act was borne out of the realization that legislation was required to criminalize computer related offenses. The cyber crime provisions contained in the ECT Act are rooted in the proposals of the Law Commission. The main focus of this research paper is section 86 of the ECT Act. Section 86 states the following:

> *Section 86 of the Electronic Communications Act on unauthorized access to, interception of or interference with data::*
>
> 1) *Subject to the Interception and Monitoring Prohibition Act 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so is, guilty of an offence.*
> 2) *A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.*
> 3) *A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use distributes or possesses any device, including a computer program or component, which is designed to primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, or access code or any other similar*

[9] Van der Merwe (n 2)

kind of data with the intent to unlawfully utilize such item to contravene this section, is guilty of an offence.

4) *A person who utilizes any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, guilty of an offence.*
5) *A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, of service to legitimate users is guilty of an offence.*

The ECT Act has provisions relating to the access, interception or the interference with data. It effectively deals with the crimes of "hacking" and "cracking". As the statistics have shown, these crimes have become prevalent over the years.[10] The ECT Act also defines computer-related extortion, fraud and forgery. It also contains provisions relating to attempt, and aiding and abetting. These provisions restate the ordinary criminal law.

Special interception legislation is also in force in South Africa. The provisions dealing with unauthorized access to and interception of data[11] are subject to the Interception and Monitoring Prohibition Act.[12] The purpose of the Act is to both prohibit the interception and monitoring of certain communications and to provide for authorization to do so in certain circumstances. Offences and penalties are provided for violation of the Interception Act's general provisions. The Regulation of Interception of Communications

[10] http://www.securitystats.com/infosec.html
[11] Section 86 (1) Electronic Communications Act No. 25 of 2002
[12] Interception and Monitoring Prohibition Act No. 127 of 1992

and Provision of Communication-related Information Act is the IMIP Act's successor in title. However, it has not yet been proclaimed in the Government Gazette.

There are further crimes that are provided for in the Electronic Communications Act. These are, among others, falsely claiming to be an accredited offeror of authentication products or services[13], falsely claiming to be a recognized foreign offeror of authentication products or services.[14] An offence is also committed when a critical database administrator does not take remedial action under section 58 (1) ECT Act.[15] Furthermore, not cooperating with a cyber inspector is also a crime under the Act.[16]

However, there are important crimes that are not in the Electronic Communications Act. These are phishing, advance fee fraud, identity theft and cyber stalking to name a few. These omitted offences will be discussed at length in the research paper.

1.3 International Law

The international community drafted legislation to effectively deal with the problem of computer-related crime. The signatory states have agreed to the Council of Europe Convention on Cybercrime (Cybercrime Convention).[17] Although South Africa is one such signatory, we have not ratified the Convention. The ECT Act and the Regulation of

[13] Section 37 (3) Electronic Communications Act No. 25 of 2002
[14] Section 40 (2) Electronic Communications Act No. 25 of 2002
[15] Section 58 (2) Electronic Communications Act No. 25 of 2002
[16] Section 82 (2) Electronic Communications Act No. 25 of 2002
[17] Council of Europe's Convention on Cybercrime 23 2001 (ETS No 185) available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Interception of Communications and Provision of Communication-related Information Act contains substantive criminal and procedural law provisions that can be found in the Convention agreed to by the Council of Europe. The Convention deals with offences against the confidentiality, integrity and the availability of computer data and systems. It also addresses issues such as jurisdiction, principles relating to extradition, international cooperation and search and seizure.[18]

There is Additional Protocol to the Convention on Cybercrime. [19] European Committee on Crime Problems (CDPC), are a committee of experts on the criminalization of acts of a racist or xenophobic nature committed through computer systems. It was found that there was a need for such protocol. The protocol defines the following offences: the dissemination of racist and xenophobic material through computer systems[20], a racist and xenophobic motivated threat[21], a racist and xenophobic motivated insult[22], and the denial, gross minimization, approval or justification of genocide or crimes against humanity.[23] The protocol has been open for signature since November 2002. However, it is not in force as yet.

The Organization for Economic Cooperation and Development (OECD)[24] drafted the Guidelines for Security of Information Systems. The OECD expects states to establish a

[18] Cybercrime Convention (n 17)
[19] Additional Protocol to the Convention on Cybercrime (ETS No 189) available at http://www.legal.coe.int/economiccrime/cybercrime/AP_Protocol(2002)5E.pdf
[20] Article 3
[21] Article 4
[22] Article 5
[23] Article 6
[24] The Organization for Economic Cooperation and Development (OECD) available at www.oecd.org

new policy or amend existing policy with regard to the protection of information systems and networks according to the nine principles in the guideline.[25]

1.4 Jurisdiction

1.4.1 Crimes committed in South Africa

The possible problem of the court's jurisdiction in electronic crime situations has been preempted by section 90 of the ECT Act. Section 90 of the ECT Act sets out the jurisdiction of the courts in electronic crime cases.

Section 90 of the Electronic Communications Act[26] states the following:

> *1) A court in the Republic trying an offence in terms of the Act has jurisdiction where –*
>
> *a) the offence was committed in the Republic;*
>
> *b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;*
>
> *c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or*

[25] Guidelines for Security and Information Systems available at http://www.oecd.org/dataoecd/27/6/2494779.pdf

[26] Electronic Communications Act No. 25 of 2002

d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

Various factors have to be taken into account in order to determine which court will have the necessary jurisdiction to hear the matter. The underlying principle which permeates throughout the rules relating to jurisdiction is that the court with jurisdiction must be empowered to ensure that its orders are carried out. Section 90 states the various grounds of jurisdiction a court could have. These grounds will be considered in turn.

A crime that was committed in the Republic falls within the jurisdiction of South African courts.[27] The individual need not be a citizen or a permanent resident of South Africa. It is sufficient that the offence was committed in this country.

Section 90 (1) (b) states that the courts have jurisdiction where any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic. It is unclear as to what type of action constitutes "preparation" for a crime. It is possible that the wording of the section is wide enough cover situations where the plans to commit the crime were made in South Africa. The court may preside over a case where the accused prepared the offence from within the borders of South Africa.

[27] Section 90 (1) (a) Electronic Communications Act No. 25 of 2002

Furthermore, any part of a computer-related offence that is committed in this country may be resided over by a South African criminal court. It could be said that "part" of an offence could either be planning or the execution of that offence.

Section 90 (1) (b) also applies to situations where the offence committed had an effect in the Republic. The court has jurisdiction over the matter notwithstanding the physical location of the accused. The effect of the crime may be felt by individuals, juristic persons such as municipalities, bodies corporate, companies, close corporations and the State. Examples of impact of the crime could be a defaced website or the suffering of losses by a company.

Section 90 (1) (c) of the ECT Act states that the court has jurisdiction over an offence that was committed by a South African citizen or a person with permanent residence[28] in South Africa. The jurisdiction exists notwithstanding the country from where that person operates. In other words, the perpetrator may be located almost anywhere in the world. If a South African citizen or a permanent resident commit a crime that has an impact in South Africa, then the courts have two grounds for jurisdiction. One is by virtue of their citizenship or permanent residency. The other jurisdictional ground is covered by section 90 (1) (b) which states that the court has authority if the effect of the crime was felt in the Republic. If the accused has no citizenship or permanent residence then such an

[28] A permanent resident is one who has permit issued in terms of the Immigration Act No. 13 of 2002. A permanent resident has all the rights and privileges, duties and obligations of a citizen save for those which the law or the Constitution ascribes to citizenship: section 25 (1) Immigration Act.

individual is covered by section 90 (1) (a) which covers situations where the offence was committed in the Republic.

Section 90 (1) (c) grants the courts jurisdiction over a person carrying on business in the Republic. This is notwithstanding his or her physical location. The meaning of "carrying on business" as it is used in the legislation is of importance. A business is defined as almost anything which is an occupation or duty which requires attention.[29] The voluminous case law indicates that there should be some regularity in conducting affairs at a particular place, usually but not necessarily for profit.[30] In order to "carry on" a business a degree of continuity is necessary. Normally, an isolated transaction does not constitute carrying on a business. The isolated act of selling, with or without an intention to make profit, is not normally regarded as "carrying on business".[31] What is necessary to constitute a business is a definite intention to sell and supply something and to carry on similar acts from time to time. Alternatively, the acts must be carried out successively with the intention of carrying it on so long as it is thought desirable.[32] In R v Silber[33] where an isolated transaction was for the purposes of criminal provisions of the Workman's Compensation Act was held to be a "business transaction" as opposed to the continuous transactions or activities implicit in the notion of "carrying on business".

[29] As per Lindely L.J in Rolls v Miller (1884) 27 Ch.D. 71 (C.A.) 88 It should be mentioned that 'business' is wider than 'trade' See SA Flour Millers' Mutual Association v Rutowiz Flour Mills Ltd 1938 CPD 199 at 204; Valkin and Another v Daggafontein Mines Ltd. and Others 1960 (2) SA 507 (W)
[30] Cape Town Municipality v Clarensville (Pty) Ltd 1974 (2) SA 138 (C) 248
[31] Modderfontein Deep Levels Ltd. And Another v Feinstein 1920 TPD 288 at 290
[32] Shaw v Benson, 52 L.J.Q.B 575 at 578
[33] 1938 T.P.D 561 at 563

The court also has jurisdiction where the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.[34] In other words, the court has jurisdiction where the offence was committed on a ship[35] or an aircraft on flight or on voyage between two South African destinations. It also encompasses cases where the offence was committed on a ship or aircraft on voyage or flight to or from South Africa notwithstanding the fact that the aircraft or ship was not registered in South Africa.

1.4.2 Crimes Committed Outside South Africa

E-crimes may be committed by someone outside of South Africa's borders. Assuming that a perpetrator has violated provisions of the ECT Act, the South African authorities would have to secure the co-operation of crime enforcement authorities in other countries. This would involve the arrest and the extradition of the individual accused of the crime. The extradition of the individual is only possible where the crime committed by the person is also a crime in the country where he or she is currently located. Conversely, if the offence that he or she has committed is not a crime in the country where they have taken up residence, then unfortunately, that person cannot be extradited to South Africa for prosecution.

[34] Section 90 (1) (d) Electronic Communications Act No. 25 of 2002
[35] Harris DJ Cases and Materials on International Law Ships (2004) 439 states that ships are deemed to have a nationality for international law purposes. Normally, a ship is registered under the law of a particular state and is then, under that state's law, both entitled to fly its flag and deemed to have its nationality.

South Africa's Extradition Act defines 'extraditable offence' as an offence punishable by deprivation of liberty for six months or more.

Chapter 2

Unlawful Access and Interception

Large and small businesses, government computer networks as well as home computer owners have all been targeted by organized criminal syndicates and radical hacking groups. Furthermore, fundamentalist hacking activity is rising and has been getting more sophisticated over the last three years. A number of hacking groups from Kashmir, Pakistan, Morocco, Turkey, Chechnya, Saudi Arabia, Kuwait, Indonesia and Malaysia are collaborating both with each other and a fringe of anti-globalization groups based in the West in order to target international and domestic online assets.[36] In South Africa, more than 60 websites were defaced on 17 July 2003. This is a new daily record and it is significantly higher than that of the previous record of 52 websites defaces in a 24-hour period.[37] The illegal interception of data is also common and its impact is felt by government, businesses and home computer owners alike. The object of this part of the paper is to examine the Electronic Communications Act's response to the scourges of unlawful access and interception of data. References to the Cybercrime Convention will be made in order to aid with the interpretation of section 86 (1) of the ECT Act.

2.1 General Overview of Section 86 (1)

[36] Matai DK 'Cyberland Security: Organised Crime, Terrorism and the Internet' available at http://www.oii.ox.ac.uk/collaboration/lectures/20050210_matai_speech_v1.0_web.pdf
[37] Leggat H 'Hackers Have a Free Ride in South Africa' available at http://estrategy.co.za/article.asp?pklArticleID=2542&pklIssueID=453&pklCategoryID=131

Section 86 (1) of the ECT Act is in part a reflection of Article 2 of the Cybercrime Convention on Illegal Access. Article 2 of the Convention reads as follows:

> *Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data*[38] *or other dishonest intent, or in relation to a computer system that is connected to another computer system.*[39]

The Explanatory Report to the Convention suggests that access may be illegal where the perpetrator infringed security measures with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.[40] Under the ECT Act, the issues of unauthorized access[41] and devices that are used to overcome security measures[42] are dealt with in separate sections. Despite this slightly different approach, ECT Act still embodies the spirit and purport of the Convention.

[38] Cybercrime Convention defines computer data as any representation of fact, information or concepts in a form suitable to cause a computer system to perform a function.
[39] Article 2 Cybercrime Convention
[40] Article 2 Cybercrime Convention
[41] Section 86 (1) Electronic Communications Act No. 25 of 2002
[42] Section 86 (5) Electronic Communications Act No. 25 of 2002

Section 86 of the Electronic Communications Act on the unauthorized access to, the interception of or the interference with data states the following:

1) *Subject to the Interception and Monitoring Prohibition Act 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so is, guilty of an offence.*

Section 86 (1) of the ECT Act is subject to the Information and Monitoring Prohibition Act (IMIP Act). Under this section, a person may not unlawfully access or intercept data stored on a computer. The person who authorises or permits the accessing or interception of the data may either be a natural person or a juristic person such as a company or a university.

The Information and Monitoring Interception Prohibition Act came into operation prior to the Electronic Communications Act. The IMIP Act was promulgated in 1992. It is arguable that the use of the internet was not as widespread in 1992 as it is today. The IMIP Act applies to the interception and monitoring of communication that takes place over the web.

The Regulation of Interception of Communications and Provision of Communication-related Information Act[43] (RICA) is the IMIP Act's successor in title. The RICA was signed on 30 December 2002 and it will come into operation on a date to be fixed by the

[43] Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002

President by proclamation in the Government Gazette. Upon commencement, the RICA will repeal the IMIP Act. Until that date, the provisions of the RICA will remain an academic interest. For the purposes of this research paper, both the IMIP Act and the RICA will be referred to.

2.2 Interpretation of the Section 86 (1)

Section 86 (1) ECT Act criminalizes the unauthorized access of or the interception of data stored on computers. Data is defined as electronic representations of information in any form.[44] Section 86 (1) does not seek to protect the physical computer itself but rather the information that is stored on the machine or the data being transmitted on the telecommunications line.

Likewise, "illegal access" in the Cybercrime Convention covers the basic offence of dangerous threats to and attacks against the security of computer systems and data. It seeks to protect the confidentiality, integrity and availability of data.[45]

The word "access" as it is used in the Convention comprises the entering of the whole or any part of a computer system. This may be the computer hardware, components, stored

[44] Section 1 Electronic Communications Act No. 25 of 2002
[45] Explanatory Report to the Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

data of the system installed, directories, traffic and content-related data. However, it does not include the mere sending of an email message or file to that system.[46]

Section 86 (1) of the ECT Act is fairly similar to Article 2 of the Cybercrime Convention. Parties to the Cybercrime Convention are obliged to criminalize the illegal access of data. Under the Convention, a person who intentionally and "without right" accesses a computer system is guilty of an offence. "Without right" means that the owner or other right holder of the system or part of it did not consent to the accessing of the data.[47] On the other hand, section 86 (1) of the ECT Act refers to the intentional access to data without permission or authorization. The accessing of data without permission or authorization implies that the access to the data was without right.

The ECT Act does not define the word "access" and the phrase "without authority or permission". A question arises as to why the legislature did not define these terms. In the absence of such an answer, it could be assumed that the legislature did not feel the need to define "access" and the term "without authorization" because they saw them as self-explanatory. It is arguable that there are varied opinions on the ease of defining these terms. An American court in United States v Morris[48] for example, rejected the defendant's request for jury instruction on the definition of "authorization" on grounds that the word is of common usage and without any technical or ambiguous meaning.

[46] Explanatory Report on the Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
[47] Explanatory Report on the Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
[48] United States v Morris, 928 F.2d 504, 511 (2d Cir. 1991) Recent court decisions have begun to acknowledge some difficulties in defining without authorization see e.g. EF Cultural Travel BV, 274 F 3d at 582 Congress did not define the phrase "without authorization: perhaps assuming that the words were obvious. However, the meaning has proven to be elusive.

However, these terms are not as self-defining as they may appear to be. Getting to grips with the meaning of these terms is pivotal to understanding the type of conduct that is punishable under the ECT Act.

A statute without definitions means that the courts are tasked with finding an appropriate definition. A proposal could be made for the courts to interpret "without authority" in ECT Act to mean, among other things, a breach of contract that governs conduct between parties. The contract could be embodied in the terms and conditions of a website for example. Accessing the website in violation of the terms and conditions would amount to access "without authority".[49]

There may be situations where a person authorizes the use of their computer thus making the use of that computer 'lawful' so to speak. However, being granted permission to use the computer does not necessarily imply that there is permission to access or to intercept all the data on that computer. Therefore, an accused cannot argue that he or she should not be found guilty of an offense because they did not make use of the computer itself without permission. It goes without saying that hackers have the ability to access data without physical access to the computer on which it is stored. The ECT Act, the IMIP Act and the RICA do not seek to criminalize the unauthorized use of a computer but rather the unauthorized access or interception of protected data stored on computers being transmitted via the telecommunications line.

[49] America Online v LCGM Inc. 46 F. Supp. 2d 444 (E.D. Va. 1998) 450

The definition of 'interception' as it is used in the ECT Act is of importance too. Although the IMIP Act does not define 'interception', the dictionary defines it as preventing something from preceding or arriving.[50] The interception may take place by means of a monitoring device. A monitoring device is defined by the Interception and Monitoring Prohibition Act as any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment to listen to or to record any conversation or communication.[51]

The RICA, on the other hand, does define 'interception'. It means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of the communication available to another person other than the sender or recipient or intended recipient of that communication. It includes the monitoring of any such communication by means of a monitoring device, the viewing, examination or the inspection of the contents of any indirect communication and the diversion of any indirect communication from its intended destination to any other destination.[52]

Section 2 (1) (a) of the Interception and Monitoring Prohibition Act prohibits any person from intentionally and without the knowledge or permission of the dispatcher intercepting a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line.

---

[50] The New Shorter Oxford English Dictionary (1993) 1391 defines 'interception' as to prevent, hinder, to obstruct so as to prevent from continuing to a destination; to stop in course of a journey.
[51] Section 1 Interception and Monitoring Prohibition Act No. 127 of 1992
[52] Section 1 Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002

The RICA also prohibits an unauthorised person from intentionally intercepting or attempting to intercept or authorise or procure any other person to intercept any communication in the course of its occurrence or transmission.[53] It is also important to note that the RICA criminalises the mere attempts to do these things. This implies that even failed interception may be punishable. It emphasises the importance placed on punishing the perpetrators of the crime whether or not they were successful in their outcome.

The subject of unauthorised interception of data is fairly topical across the world. Generally speaking, section 86 (1) of the ECT Act, the IMIP Act and the RICA take a firm stand against illegal interception. Article 3 of the Cybercrime Convention also deals with the issue in a comparable fashion. Article 3 states the following:

> Article 3 – Illegal Interception
>
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committee intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest*

[53] Section 2 Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002

intent, or in relation to a computer system that is connected to another computer system.[54]

Article 3 aims to protect the right of privacy of data communication. The offence that it establishes applies to all forms of electronic data transfers, whether by means of telephone, fax, email or as a result of a file transfer.[55] Likewise, the ECT Act on interception applies to data in any form. Interception by "technical means" refers to the use of monitoring devices and such like.

The offence in Article 3 relates to the "non-public" transmission of data. The term "non-public" qualifies the nature of the transmission or the communication process. It does not relate to the nature of the transmitted data. Although the data communicated may be publicly available information, the parties may wish to communicate confidentially. Furthermore, data may be kept secret for commercial purposes until the service is paid.[56] Therefore, the term non-public does not per se exclude communications over public networks.[57] Likewise, section 86 (1) of the ECT Act seeks to protect data that is generated by any person be it a company, government or an individual. The ECT Act also seems to recognize that these persons should opt to divulge their data or information when it suits them. Illegal access or interception of the data is therefore a punishable offence.

[54] Article 3 Cybercrime Convention
[55] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
[56] Take for example Pay-TV.
[57] Explanatory Report on Cybercrime Convention http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

2.3 Elements of the crime

2.3.1 Intention

The ECT Act refers to the intentional access or interception of data without authority or permission to do so. Criminal law recognizes that there are different types of 'intention'. Some of these are *dolus directus, dolus indirectus* and *dolus eventualis*. *Dolus directus* is present where the accused's aim and object was to carry out the unlawful act or to cause the consequence even though the chance of its resulting was small.[58] *Dolus indirectus* is where, although it is not the accused's aim and object, he or she foresaw the unlawful act or consequence as certain, or as substantially certain.[59] *Dolus eventualis* exists where the accused does not mean to bring about the unlawful circumstances or to cause the unlawful consequence which follows from his or her conduct. However, he or she foresees the possibility of the circumstance existing or the consequence ensuing and proceeds with his or her conduct.[60]

The use of the word 'intention' in a statute indicates the requirement of dolus.[61] However, the use of the word 'intention' does not necessarily imply that *dolus*

[58] Burchell J and Milton J *Principles of Criminal Law* (1997) 301
[59] Burchell and Milton (n 58) 301
[60] Burchell and Milton (n 58) 302
[61] In S v Nxumalo 1993 (3) SA 456 (O) (1993 (1) SACR 743) the Court concluded that *mens rea* in the form of intention was required for a contravention of the Copyright Act 98 of 1978, since the statute resembled the common-law crimes of theft and fraud which could not be perpetrated negligently.

eventualis will be sufficient for liability. Certain offences created by statute have been held to require *dolus directus* rather than *dolus eventualis*.[62]

Although the ECT Act specifically requires intention for the act to be a punishable offense there appears to be no indication of what type of intention is required. An argument could be made for the scope of the intention to cover those people who go out of their way to cause the unlawful consequence. On a plain reading of the text, *dolus directus* should be the standard of intention that the courts could use. It could be argued that any other type of intention could lead to absurd results that could not have been the intention of the legislature. Take for example an innocent employee who is granted permission to make use of his superior's computer. In this particular work environment, access to certain data is restricted because of workplace policy. If for some reason, other than the employee's direct intention, the protected data pops up on the screen, the courts may find the employee guilty of an offense if the court used either *dolus indirectus* or *dolus eventualis* as a standard.[63] In short, it is argued that the courts should limit the interpretation of the word 'intention' in this context to *dolus directus*. This is to prevent absurd results from ensuing such as the conviction of persons who had no direct intention to access or to intercept the protected data.

[62] Burchell J *Principles of Criminal Law* (2004) 501

[63] The information does not need to be accessed or intercepted in a complicated way. The level of technology used to secure the data does not define the sensitivity of the information. It is sufficient that the data is classified as confidential and therefore off limits to unauthorized personnel.

It is also important to bear in mind that in South African law, the general rule is that an act does not make a man guilty unless his mind is also guilty.[64] In construing statutory prohibitions or injunctions the legislature is presumed, in the absence of clear and convincing indications to the contrary, to have intended innocent violations thereof to be punishable.[65] In other words, it is to be presumed that the legislature intended *mens rea* to be an element of liability of a statutory offence. The presence of fault words such as 'maliciously', 'knowingly' or 'corruptly' are somewhat indicative of the legislatures intention to not punish innocent violations of the legislation. An argument could be made for the court not to punish innocent violations if the offense requires *dolus directus*. Although the ECT Act specifically requires intention there appears to be no indication of what kind of intention is required. The scope of the intention should cover those who go out of their way to cause the unlawful consequence.

An accused individual would be guilty of the offense regardless of their motives. To require motive to qualify the intention is fairly restrictive. Motive is a person's reason for conduct. It is something separate and distinct from intention. The general rule is that motive is not taken into account when determining criminal intent. The reason for disregarding motive when determining criminal liability is

[64] *Actus non facit reum nisi mens sit rea*

[65] As per Botha JA in S v Arenstein 1964 (1) SA 361 (A) 365 This case has been cited in recent judgments: Amalgamated Beverage Industries Natal (Pty) Ltd v Durban City Council (1994 (3) SA 170 (A) SACR 373); Scagell v Attorney-General, Western Cape 1997 (2) SA 368 (CC) (1996 (2) SACR 579); Epstein v Bell 1997 (1) SA 483 (D)

that individual motives are too complex and are sometimes too obscure to provide a reliable basis for determining liability for punishment.[66]

An accused is culpable of the offense of prohibited access or interception where he or she had intent. This implies that the accused must have had the intent to obtain access to or to intercept the computer data. He or she must also have had knowledge of the unlawfulness of his or her conduct. Because the crime requires *mens rea* in the form of intention liability is now invariably dependent upon the accused having known that he was acting in contravention of the law. It is not necessary to prove that the accused knew the detailed requirements of the offence charged, the exact section or wording of the legislation or the penalty for the offence, but merely that he or she knew, or at least foresaw the possibility, that what he was doing was contrary to law in the broad sense.[67] To put it another way, the accused must have had known or suspected that he or she had no authority to access or to intercept the data on the computer. The knowledge component of the intent should be interpreted sufficiently widely to include cases where the accused turns a blind eye to the unlawfulness of their conduct.

2.3.2 Unlawfulness

The unlawful element of the crime is defined by the absence of permission or authority to access or to intercept the data. The authority must come from the

[66] Burchell (n 62) 463
[67] Burchell (n 62) 497, 498 See also S v Hlomza 1987 (1) SA 25 (A) 31, 32

owner or the person lawfully in charge of the data.[68] A distinction should be drawn between the person with authority to use computer and the person with authority to use the data. In this regard it must be noted that it is not the permission of the person in charge of the computer that is required but rather the permission of the person in charge of the data.[69]

The absence of authority is an objectively determinable element. It will be determined with reference to the facts of each particular case.[70] Authority is usually derived from the authorization by or the permission of the principal. Authorization is a unilateral juristic act by which one person empowers another to act on his behalf.[71] Authorization confers actual authority in general or specific terms, expressly or tacitly.[72] The person authorized to use the data or software program must have authority to delegate the authority to someone else. The person who delegates this authority to someone else cannot exceed authority given to him or her.

The issue of authorization may arise in an employer-employee context. Take for example an employee who secures company data or information that he or she has authority to access on a day to day basis in the course of or for the purposes of his employment. Assume that the employee intends to procure this data for his or her

[68] Access or interception of data without the permission of an owner's username and password is illegal
[69] South African Law Commission (n 6)54
[70] Cf. Dicks v South African Mutual Fire and General Insurance Co Ltd 1963 4 SA 501 (N) 504 et seq
[71] Maasdorp v The Mayor of Graaff-Reinet 1915 CPD 636 639
[72] Van der Merwe et al *Contract: General Principles* (1993) 178 See also Coetzer v Mosenthals Ltd 1963 4 SA 22 (A)

own advantage or for the advantage of a third party. In these circumstances, is the access to the data without authorization? The court in Shurgard Storage Centers Inc v Safeguard Self Storage Inc[73] was faced with this very situation. The employee acquired the employer's company trade secrets for a rival company. The said employee was charged with intentionally accessing the plaintiff's computer without authorization.[74] The court found that the authorization of an employee ended when that employee began acting as an agent for another person other than the employer.[75] The court concluded that the conduct of the employee was without authorization.[76] The case has the effect of criminalizing conduct that is not work-related. For this reason, it is submitted that employers set out data-usage policies or workplace policy documents that stipulate what is expected of employees in the realm of data and computer usage.

On another note, an accused may refute the allegations of the unlawfulness of his or her access or interception by demonstrating any one of the following things stipulated in the RICA: Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.[77] Alternatively, interception may take place if one of the parties to the communication has given prior consent in writing to such interception, unless

[73] 119 F. Supp. 2d 1121 (W.D. Wash. 2000)
[74] 118 U.S.C.§1030 (a) (2) (c)
[75] Shurgard case (n 73) 1124
[76] Shurgard case (n 73) 1125
[77] Section 4 (1) Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002

such communication is intercepted by such person for purposes of committing an offence.[78]

On the issue of interception, a person in the course of carrying on a business may intercept any indirect communication. The communication should be the means by which a transaction is entered into in the course of the business. It could also be communication that otherwise relates to that business or which takes place in the course of the carrying on of that business in the course of its transmission over a telecommunication system.[79] Indirect communication includes email, faxes and telephonic conversations. The systems controller must have expressly or impliedly consented to the interception of the indirect communication. The purpose of such interception must be to establish the existence of facts.[80] It is not certain whether the interception of indirect communications by the systems controller will be unlawful if there is no prior written consent of the employee. In light of this vagueness, it is advisable that the systems controller obtains the written consent of its employees, if the case may be, before such interception takes place. It is also highly advisable for a juristic person to compile a clear, up-to-date, well-publicised and active policy document that sets out the permitted and/or prohibited conduct in computer and internet usage. This should be done so as to avoid criminal liability as well as the possibility of being penalised.

[78] Section 5 (1) Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002
[79] Section 6 (1) Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002
[80] Section 6 (2) Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002

As an aside, some juristic persons make use of blocking and filtering software products or devices. These software products allow the censorship of incoming and outgoing email and or prevent access to certain websites. The question to answer is whether the operation of blocking and filtering software amounts to the interception of indirect communication.

Blocking software examines and inspects the content of messages and websites to determine if it contains a set of pre-determined keywords or phrases such as 'sex' or ‘pornography’ for example. If an email and its attachments or a webpage contains one of these keywords or phrases, the message is blocked and/or deleted. In some cases a return message is addressed to the sender, informing him or her that the email was blocked. The examination and inspection of direct communication such as email or the monitoring of internet usage amounts to interception and therefore brings the conduct of the system controller into the prevue of the IMIP Act, the RICA and the ECT Act. Thus it may be argued that the use of blocking and filtering software products or devices will be unlawful where consent of the employee for instance has not been obtained.

Chapter 3

Interference with Data

The compilation of data takes time, effort and resources. Section 86 (2) of the Electronic Communications Act seeks to protect the data of persons so as to allow the enjoyment of that data without hindrance or obstruction. The main objective here is to give a general indication of how the ECT Act accomplishes this. References to Article 4 of the Cybercrime Convention will be made to assist in the interpretation of section 86 (2).

3.1 General Overview of Section 86 (2)

Article 4 of the Cybercrime Convention and section 86 (2) of the ECT Act deal with the interference of data. Article 4 states the following:

> Article 4 of the Cybercrime Convention on Data Interference
>
> 1. *Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
> 2. *A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.*[81]

[81] Article 4 Cybercrime Convention

Article 4 of the Convention obliges Parties such as South Africa to criminalize the illegal interference of data. Section 86 (2) of the Electronic Communications Act does just that.

Section 86 (2) ECT Act on the interference of data states the following:

2) *A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.*

As stated above, section 86 (2) of the ECT Act seeks to protect the data of persons so as to allow the enjoyment of that data without interference. The section makes it an offence to intentionally interfere with another person's data without authority. Any deliberate and unauthorized interference which results in the modification, the destruction or the ineffectiveness of the data in anyway is specifically prohibited by the Act.

3.2 Interpretation of Section 86 (2)

The Cybercrime Convention's reference to the "damaging" and "deterioration" relates to the negative alteration of the data. The Explanatory Report to the Convention informs us that "deletion" is the destruction and the suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or to the data carrier on which it is stored. The term "alteration" means the modification of existing data. The input of malicious codes such as viruses and Trojan horses is covered under this paragraph.

Interpreting section 86 (2) of the Electronic Communications Act is a little more difficult. This is because the legislature did not provide direction on how to go about interpreting the section. The words 'modification', 'destruction' and the phrase 'rendered ineffective' form essential components of the offence. The lack of guidance in the legislation leaves us to turn to the courts for a way forward. However, seeing as section 86 (2) has yet to be adjudicated upon, general definitions of these terms will have to suffice.

Generally speaking, the interference of data is the tampering, meddling or the frustration of a person's use of that data. It is put forward that the ECT Act considers it an offence to meddle with the data of another person in a way which causes their data to be altered in form or character, to spoil the data or to cause it to become ineffectual. A person who, intentionally and without authority causes data to become ineffective is one who has caused that data not to produce the effect that the owner intended. The activities described above brings these conducts into the ambit of the section 86 (2) of the ECT Act.

Under Article 4 of the Convention, a Party may reserve the right to require that the conduct described result in serious harm.[82] The Electronic Communications Act does not contain a provision to this regard. It is arguable that the absence of such a provision widens the scope of the legislation to encompass both serious and not-so-serious offences. In order for South Africa to reserve the right to require that the offence result in

[82] Article 4 Cybercrime Convention

serious harm, we would have to notify the Secretary General of the Council of Europe of this intended interpretation.[83]

3.3 Elements of the Crime

3.3.1 Intention/Culpability

An accused is culpable of the offence of unlawfully interfering with data where he or she had the intention to do so. It is a requirement that the accused know that his or her conduct is unlawful. This does not mean that the accused should have detailed knowledge of the law that he or she is breaking as it is sufficient that the accused knew, or at least foresaw the possibility that what he was doing was contrary to the law in the broad sense.[84] To put it another way, the accused must have known or suspected that he or she had no authority to interfere with the data. The knowledge component of the intent should be interpreted sufficiently widely to include cases where the accused turns a blind eye to the unlawfulness of their conduct.[85] An accused would be guilty of the offence regardless of their motives.

As an aside, computer viruses are the bane of the data stored on computers. Every now and again, computer viruses are spread throughout various networks causing

[83] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
[84] Burchell (n 62) 497, 498 See also S v Hlomza 1987 (1) SA 25 (A) 31-2
[85] South African Law Commission (n 6) 57

damage to computers and/or data stored on these machines. [86] The question that needs to be answered is whether writing and spreading a computer virus could constitute an offence in terms of the ECT Act.

A computer virus may directly or indirectly infect a computer and/or its data and spread throughout a network. The virus tends to spread indiscriminately and could bring a network system to its knees within minutes. The parasitic nature of a computer virus is such that it either causes the computer to come to a standstill, causes programs to run irregularly and to damage or destroy files. All these consequences indicate the ways in which viruses cause data to be modified, destroyed or otherwise rendered ineffective.

Viruses are created by people who know how to write computer programs. This demonstrates that the bug is neither accidental nor a computer glitch. The intentional writing of a computer virus satisfies the requirement of intention to commit the crime of unlawful interference of data. There are times when the writers of computer viruses have a specific target in mind. However, viruses have been known to spread easily regardless of the writer's goal. With this in mind, an argument could be made for the courts to interpret the word 'intention' in section 86 (2) of the ECT Act to mean *dolus indirectus*. This is because although the perpetrator had a specific target in mind he or she must have foreseen the possibility of interfering with the data stored on other computers.

[86] Sophos reports that the following are the top ten viruses for 2004 are Netsky - P, Zafi – B, Sasser, Netsky – B, Netsky – D, Netsky – Z, MyDoom – A, Sober – I, Netsky – C, Bagle – AA. Available at www.sophos.com or http://news.bbc.co.uk/1/hi/technology/4105007.stm

3.3.2 Unlawfulness

The act of interfering with data in a way which causes the data to be modified, destroyed or otherwise rendered ineffective is unlawful only if such an act was without the authorization of the owner of the data. The keyword here is "authorization". The absence of authority is an objectively determinable element. It will be determined with reference to the facts of each particular case.[87] Authorization implies that the act of interfering with data will not be a punishable offence if such interference was authorized by the person lawfully in charge of the data. A distinction should be drawn between the person with authority to use the data and the person lawfully in charge of the data.

The case of Fugarino v State[88] illustrates the importance of making the distinction between owner of data and person authorized to use it. In this case, Fugarino was a computer programmer and an employee of the owner of the data he worked on. Part of his job involved writing programs that the employer could use. It may be assumed that in the normal course of his employment he was permitted to destroy programs where appropriate. A dispute arose between Fugarino and his employer. Fugarino decided to destroy a program he had written for his employer. The court found that the deletion of the program was without authority because Fugarino did

[87] Cf. Dicks v South African Mutual Fire and General Insurance Co Ltd 1963 4 SA 501 (N) 504 et seq
[88] 531 S.E. 2d 187 (Ga. Ct. App. 2000)

not have the permission to do so from the owner of the company. [89] The court looked at the way in which Fugarino had destroyed the data and found that the vindictive and retaliatory manner of the employee constituted conduct without authority.[90]

It is important that the authority comes from the person lawfully in charge of the data for another reason. There may be situations where a person other than the owner of the data has authority over that data. For example, in a criminal law matter the investigating authority may charge that certain data in the possession of an individual or juristic person should not be interfered or tampered with. The tampering of data in this situation in a way which causes such data to be modified, destroyed or otherwise rendered ineffective may be a criminal offence and it may constitute an obstruction of justice. In this situation, the authority shifts from the owner of the data to the investigating authorities who may be seen as the persons lawfully in charge of the data.

[89] Furgarino case (n 89) 189
[90] It could be argued that the court took into account the motive of the employee here.

Chapter 4

Overcoming E-Security Measures

It is unfortunate that there has been a proliferation of network security breaches over the past few years. A survey conducted by the Computer Security Institute found that of the 643 corporations that they surveyed, over 70% reported network security breaches during the year 2000. In addition, the Computer Emergency Response Team (CERT) co-ordination center at Carnegie-Mellon University reported a 183% increase in reported incidents between 1998 and 1999. CERT also reported an increase from 9 859 incidents in 1999 to 15 162 incidents in the first three quarters of the following year.[91]

The common sale, production and usage of these items are a cause for concern for anyone conducting any sort of business or transaction over the internet. Section 86 (3) and (4) of the Electronic Communications Act and Article 6 of the Cybercrime Convention target this very issue. This part of the research aims to discuss the measures under the Electronic Communications Act and the Cybercrime Convention.

4.1 General Overview of Section 86 (3) and (4)

Section 86 (3) and (4) of the Electronic Communications Act deals with the issue of protecting the integrity of security measures and passwords used to secure data. Section 86 (3) and (4) states the following:

[91] http://www.usdoj.gov/criminal/cybercrime/intl/USComments_CyberCom_final.pdf

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

4) A person who utilizes any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, guilty of an offence.

Section 86 (3) and (4) of the ECT Act criminalizes of the development and trafficking in devices, components and programs which are primarily used to obtain unauthorized access to restricted data protected by passwords or access codes. Such devices, components and software are sometimes designed to protect copyrighted material such as CDs, DVDs and written material. Some owners of literary works are taking technological measures to protect their intellectual property. For instance automated rights management (ARM) allows copyright owners to control the use of their work. Automated rights management provides the owners of intangible assets with defensive mechanisms built into computer hardware and software and implemented via firewalls, encryption and passwords. ARM aims at permitting information providers, and perhaps even individual owners of proprietary data, to sell access on a document-by-document basis. The simplest such pay-per-use systems offer encrypted documents for sale, or rather the keys to those

documents, one at a time. The purchaser of a key gets access to a single locked document.[92]

Similarly digital rights management (DRM) is a used to control or to restrict the use of digital media content on electronic devices with such technologies installed. Music, visual artwork, computer and video games and movies are often protected by DRM.[93] The discussion on section 86 (3) and (4) below will illustrate how our law shields protective measures such as ARM, DRM, other devices, components, software, passwords and codes. References to a United States statute, the Digital Millennium Copyright Act of 1998 (DMCA) will be made will be made as it touches on issues pertinent to this line of discussion.

Article 6 of the Cybercrime Convention contains a detailed provision on the misuse of devices. It states the following:

Article 6 - Misuse of devices

1. *Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
    a. *The production, sale, procurement for use, import, distribution or otherwise making available of:*

[92] http://www.tomwbell.com/writings/FullFared.html
[93] http://en.wikipedia.org/wiki/Digital_Rights_Management

i. *A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2- 5;*

ii. *A computer password, access code or similar data by which the whole or any part of a computer system is capable of being assessed is*

With intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5;

And

b. *The possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A party may require by law that a number of such items be possessed before criminal liability attaches.*

2. *This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.*

3. *Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).*

4.2 Interpretation of Section 86 (3) (4)

Unfortunately, the ECT Act does not provide direction where the issue of the definition of terms is concerned. For this reason it is recommended that we look towards the Cybercrime Convention to glean some ideas on how certain terms may be interpreted. The word "distribution" in the Cybercrime Convention refers to the active act of forwarding data to others, while "making available" refers to the placing online devices for the use of others.[94] The inclusion of a "computer program" in the Convention refers to programs that are, for instance, designed to alter or even to destroy data or to interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.[95]

The offence described in the Cybercrime Convention requires that it be committed intentionally and without right. In order to avoid the danger of over-criminalization where devices are produced and put on the market for legitimate purposes, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific or direct intent that the device is used for the purpose of

[94] This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices.
[95] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

committing any of the offences established in Articles 2 through to Article 5 of the Convention.[96]

It is not certain when producing, adapting, selling, distributing and the procurement of goods which are primarily designed to overcome security measures would be lawful. It is arguable that the word "unlawfully" as it is used in section 86 (3) of the ECT Act qualifies these activities. It is proposed that section 86 (3) and (4) of the ECT Act could be interpreted in a manner similar to the interpretation of Article 6 of the Cybercrime Convention. Under the Cybercrime Convention, it is assumed that test devices ("cracking devices") and network analysis devices that are produced for legitimate purposes and that are designed by industry to control the reliability of their information technology products or to test system security, and would be considered to be lawful.[97] In light of this, it is suggested that the law enforcement authorities and research institutions that produce, use and distribute these devices should be exempt from liability under section 86 (3) of the ECT Act. It is debatable that it could not have been the intention of the legislature to prosecute these individuals. Until the courts have adjudicated on this point, the question as to whether crime enforcement authorities and researchers will be liable remains unanswered.

The Electronic Communications Act does not provide guidance on the meaning of the phrase 'designed to primarily to overcome security measures'. On a plain reading of the

[96] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
[97] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

section, the phrase could mean that the device, computer program or component's main object should be to override the security measures put in place by the owner of the data. If the device, program or component forms a part of another device then one should ask what the primary or main function of the device or program is. This means that although the device, software program or component may perform (other) legitimate functions, it would still be an offence to sell, offer to sell, procure, design or to use that portion of the device, software program or component which is solely for the purpose of circumventing security measures employed to protect data.

Section 86 (3) and (4) of the ECT Act and Article 6 of the Cybercrime Convention are restricted to devices designed or adapted primarily for the purpose of committing an offence. Nevertheless, this excludes dual-use devices. It could be argued that if the device or software program has only limited commercially significant purposes other than the circumvention of security measures then the product manufacturer, distributor and user may be found guilty of an offence as per section 86 (3) and (4) of the ECT Act.

Provisions similar to section 86 (3) of the ECT Act can be found in the Digital Millennium Copyright Act of 1998 (DMCA). The DMCA targets the circumvention of digital walls guarding copyrighted material and trafficking in circumvention tools. A simple reading of section 1201 of the DMCA makes it clear that its prohibition applies to the manufacturing, trafficking in and the making of devices that would circumvent encryption technology. It is the technology itself at issue.

The Electronic Communications Act does not define the phrase 'security measure'. It is put forward that the phrase 'security measure' in the sense used by section 86 (3) of the ECT Act is similar to the term 'technological measure' referred by in the DCMA. The DMCA defines the expression to 'circumvent a technological measure' as to 'descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate or impair technological measure, without the authority of the copyright owner'.[98] The DMCA also defines 'to circumvent protection afforded by a technological measure' as 'avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure.'[99] A brief look at the DMCA demonstrates how the interpretation of a statute is made easier when crucial terms are defined. In the absence of sufficient clarity from the legislature, it is suggested that our courts should possibly consider looking to the DMCA as well as the Cybercrime Convention for possible guidance.

There is still a question that needs to be answered in the context of devices and software used to overcome passwords and codes. The question is could an accused be successfully convicted under section 86 (3) and (4) of the ECT Act if that person did not introduce the device or program that overcame a password or code-based restriction him or herself? In other words, could a conviction ensue if the data owner's computer system already contains flaws or devices, components or software that enabled the restricted data to be accessed? This question has not been answered by our courts as yet. It could be argued that a conviction should follow where a person exploits the weaknesses in a system to

[98] Section 1201 Digital Millennium Copyright Act (3) (A)
[99] Section 1201 Digital Millennium Copyright Act (2) (A)

obtain access without authorization. The court in United States v Morris[100] coined the intended function test. In short, devices, components and software should not be used in a way that the owner of such material did not intend them to be used.[101] In light of this judgment, it is suggested that the South African courts should perhaps convict a person who obtains access to protected data using the devices, software or exploiting weaknesses in the computer of another in a way that was not intended by the owner.

As an alternative, an accused could be found guilty under the hacking and interception provision located in section 86 (1) of the ECT Act. This section simply prohibits access of data without the authority or the permission to do so.

There is yet another issue that the courts may have to address in the future. That is, could an accused be convicted of 'accessing' data restricted by a password or a code if that person was not successful in obtaining the data? This question came up in the American case of State v Allen.[102] In this case, Allen would manipulate the Southwestern Bell Telephone computer to his advantage to dial up free long-distance phone calls. It is assumed that when the computer prompted Allen for a username and password, he would guess them correctly. The State had argued for the definition of "access" to mean to approach, instruct, communicate with, store data in retrieve form, or otherwise make use of any resources of a computer.[103] The court stated that if to access a computer really meant 'to approach' then any unauthorized physical proximity to a computer could

[100] 928 F.2d 504 (2d. Cir. 1991)
[101] Morris case (n 101) 510
[102] 917 P. 2d 848 (Kan. 996)
[103] Allen case (n 103) 851 quoting Kansas Statutes Annotated § 21 – 3755 (a) (1)

constitute a crime. Furthermore, the court turned to and preferred the Webster's dictionary meaning "access". Webster's defines "access" as "freedom or ability to obtain or make use of." The Kansas court used this definition to shed light on Allen's conduct. The court came to the following conclusion:

> *Until Allen proceeded beyond the initial banner and entered appropriate passwords he could not be said to have had the ability to make use of Southwestern Bell's computers or obtain anything. Therefore, he cannot be said to have gained access to Southwestern Bell's computer systems as gaining access is commonly understood.*[104]

In short, the court held that being prompted to enter a username and password did not amount to access. However, overcoming the username and password restriction by unlawful means is access and it is a punishable offence. It is argued that our courts should possibly adopt a similar approach and bear in mind that to punish someone for coming across the username and password prompt is excessive. Adopting a broad definition of "access" in this context could lead to the absurd result of courts punishing someone for coming across a username and password prompt.

[104] Allen case (n 103) 853

4.3 Elements of the Crime

4.3.1 **Intention/Culpability**

The ECT Act refers to the intentional utilization of a device, computer program or component that is designed primarily to overcome security measures, passwords or codes. The use of the word 'intention' in a statute indicates the requirement of *dolus*.[105] In South African law, the general rule is that the conduct of the accused does not make him or her guilty unless his mind is also guilty.[106] An argument could be made for the scope of the intention to cover those people whose objective is to cause the unlawful consequence. With this in mind, *dolus directus* should perhaps be the standard of intention used by the courts when interpreting section 86 (3). *Dolus directus* is present where the accused's aim and object was to carry out the unlawful act or to cause the consequence even though the chance of its resulting was small.[107]

Criminal law does not take into account the motives of the accused. Therefore, it seems that a perpetrator would be guilty of the offence regardless of their motives. This is mainly because individual motives are too complex and they are sometimes too obscure to provide a reliable basis for determining liability for

[105] In S v Nxumalo 1993 (3) SA 456 (O) (1993 (1) SACR 743) the Court concluded that *mens rea* in the form of intention was required for a contravention of the Copyright Act 98 of 1978, since the statute resembled the common-law crimes of theft and fraud which could not be perpetrated negligently.
[106] *Actus non facit reum nisi mens sit rea*
[107] Burchell and Milton (n 58) 301

punishment.[108] Furthermore, to require motive to qualify the intention would restrict the interpretation of the statute.

As stated above, there is a measure of uncertainty that remains regarding the application of section 86 (3) of the ECT Act. It seems that the section fails to take into account the need for computer security professionals and researchers to design or use products with the capacity for system penetration. These devices, computer programs or components could be used to conduct security assessments as the need arises. According to this law, even computer forensic tools that have been designed to primarily overcome security measures for the protection of data or to perform any of those acts with regard to passwords or codes are unlawful.

In the aforementioned case of United States v Morris[109] the accused was charged with intentionally accessing a Federal interest computer without authorization.[110] Morris had written a program that was designed to uncover flaws in the internet security system. The program was designed primarily to guess passwords. However, the program caused severe damage to part of the internet which resulted in part of the internet being shut down. In his defense, Morris argued that he was not entirely "without authorization" to access the computers he had used because he had authorized access to some of those computers. The court responded as follows to this line of defense:

[108] Burchell (n 62) 463
[109] 928 F.2d 504 (2d. Cir. 1991)
[110] 18 U.S.C § 1030 (a) (5) (A)

> *Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers.*[111]

The court's response shows that even people with authorized access overstep the mark when they access restricted data by means of a device or a program. This same line of reasoning or thinking could be applied to the ECT Act. This case more or less foretells the possible outcome of security professionals and researchers who use devices and programs to overcome restrictions on protected data unless and until exceptions or exemptions are made through amendments to the ECT Act. To neglect to do so could hinder law enforcement agencies and researchers from performing their functions.

As an aside, viruses may sometimes be used as software designed to overcome protective measures on data. It is arguable that like other forms of unpopular expression such as pornography and propaganda, the free speech provisions of the South African Constitution[112] protect even a malicious computer code. However, if the virus was programmed with the main purpose to overcome security

[111] Morris case (n 110) 511
[112] Section 16 of the South African Constitution Act 108 of 1996

measures then such programming will be illegal in terms of section 86 (3) of the ECT Act.

An accused is culpable of the offence described in section 86 (3) where he or she had the direct intention to commit the crime. The intention must be to produce, sell, offer to sell, procure for use, design, and adapt for use, distribution or possession any device, program or component that is designed primarily to overcome security precautions or passwords and codes that protect data. This means that the accused's goal must have been to commit this offence. He or she must also have had knowledge of the unlawfulness of his or her conduct. Because the crime requires *mens rea* in the form of intention liability is now invariably dependent upon the accused having known that he was acting in contravention of the law. It is not necessary to prove that the perpetrator knew the detailed requirements of the offence that he is charged with, the exact section or wording of the legislation or the penalty for the offence, but merely that he or she knew, or at least foresaw the possibility, that what he was doing was contrary to law in the broad sense.[113] To put it another way, the accused must have known or at least suspected that he or she had no authority to bypass any security measure that was installed to protect the data. The knowledge component of the intent should be interpreted widely enough to include cases where the accused turns a blind eye to the unlawfulness of their conduct.

[113] Burchell (n 62) 497, 498 See also S v Hlomza 1987 (1) SA 25 (A) 31, 32

4.3.2 Unlawfulness

The unlawful element of the crime described in section 86 (3) and (4) is defined by the absence of authority by the owner of the protected data. Only the person lawfully in charge of the data can consent to the bypassing of security measures that he or she may have put in place.

The issue of authorization to overcome security measures used to protect data was raised in the case of 321 Studios v MGM Inc. In this case, 321 Studios asserted that its software did not violate section 1201 of the DMCA because the software did not 'circumvent' encryption. 321 Studios stated that its software did not avoid, bypass, remove, deactivate or otherwise impair a technological measure, but that it simply used the authorized key to unlock the encryption. However the court held that while 321's software did use the authorized key to access the DVD, it did not have the authority to use this key as licensed DVD players do, and it therefore avoided and bypassed security measures.[114]

The absence of authority is an objectively determinable element. It will be determined with reference to the facts of each particular case.[115]

[114] 321 Studios v Metro Goldwyn Mayer Studios Inc 307 F. Supp. 2d 1085
[115] Cf. Dicks v South African Mutual Fire and General Insurance Co Ltd 1963 4 SA 501 (N) 504 et seq

Chapter 5

Denial of Service Attacks

Denials of service attacks are undesirable to say the least. These attacks interfere with the running of businesses, government computers and even personal computers. The Electronic Communications Act attempts to discourage computer users from causing denials of service. Article 5 of the Cybercrime Convention is relevant to this discussion. It will be discussed in conjunction with section 86 (5) of the ECT Act.

5.1 General Overview of Section 86 (5)

Section 86 (5) of the ECT Act garners its inspiration from Article 5 of the Cybercrime Convention. To be able to appreciate the interpretation of section 86 (5) it is suggested that Article 5 be examined. Article 5 states the following on the topic of system interference:

> *Article 5 – System Interference*
>
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.*

Section 86 (5) of the Electronic Communications Act targets the issue of denial of service attacks. It states the following:

> *5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, of service to legitimate users is guilty of an offence.*

The essential components of this offence are the intention and access to an information system with the intention to cause a denial of service to legitimate users. An information system is a system for generating, sending receiving, storing, or otherwise processing data messages and includes the internet.[116]

5.2 Interpretation of Section 86 (5)

The "hindering" mentioned to in Article 5 of the Cybercrime Convention must be serious in order to attract criminal liability. Each Party to the Convention had to determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious". For example, a Party may require a certain amount of damage to be caused in order for the hindering to be considered "serious". It seems that the drafters considered denial of service attacks as "serious".[117] It is the denial of service attacks that section 86 (5) of the ECT Act concentrates on.

[116] Section 1 Electronic Communications Act No. 25 of 2002
[117] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

Section 86 (5) of the ECT Act serves to criminalize denial of service attacks. However, the ECT Act does not provide direction on how this "attack" should be defined. A denial of service is commonly defined as an incident which deprives legitimate users or an organization of the services they would normally expect to have such as the use of email. Such an attack may even result in a website ceasing to operate temporarily. The perpetrator intentionally gains unlawful access to into a number of internet-connected computers and installs a Trojan which allows the attacker to remotely control the compromised computers. [118] He or she may purposely overload a mail server or web server with phony requests. The result is that the network is rendered unable to distinguish between legitimate traffic and malicious or false traffic during the attack and causes the mail or web server to crash.

A denial of service attack usually results in the loss of time and money for the target person or organization.

Lastly, the hindering of a computer system under the Cybercrime Convention must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are considered to be with right. These include the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar or previously installed programs. Such conduct is not criminalized by Article 5 even if it causes serious

[118] Anslie J 'Distributed Denial of Service: Internet as a War zone' available at http://www.networktimes.co.za/article.asp?pklArticleID=3202&pklIssueID=439&pklCategoryID=211

hindering.[119] Unfortunately, the Electronic Communications Act does not seem to allow for such an interpretation. There appears to be no distinction made between a person who interferes with a computer system for the purpose of research or testing for example and a person who the malicious intention of causing a denial of service regardless of the interference caused to legitimate users.

5.3 Elements of the Crime

5.3.1 Intention/Culpability

Section 86 (5) of the ECT Act refers to the intention to interfere with access to an information system so as to constitute a denial of service to legitimate users. The use of the word 'intention' in a statute indicates the requirement of *dolus*.[120] It is argued that the courts should interpret 'intention' in this case to constitute *dolus directus*. *Dolus directus* is present where the accused's aim and object was to carry out the unlawful act or to cause the consequence even though the chance of its resulting was small.[121] It could be argued that any other type of intention could lead to absurd results that could not have been the intention of the legislature. Take for example an innocent person sends email with attachments to a target person or organization. However, because of the size of the attachments the target

[119] Explanatory Report on Cybercrime Convention available at http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
[120] In S v Nxumalo 1993 (3) SA 456 (O) (1993 (1) SACR 743) the Court concluded that *mens rea* in the form of intention was required for a contravention of the Copyright Act 98 of 1978, since the statute resembled the common-law crimes of theft and fraud which could not be perpetrated negligently.
[121] Burchell and Milton (n 58) 301

person's email ceases to operate properly albeit temporarily. The conduct of the person who sent the email constitutes a denial of service attack. This is because although usually intentional and malicious, denial of service attack can sometimes happen accidentally. Interpreting 'intent' to mean *dolus directus* will help ensure that innocent people are not convicted of a crime that they had no direct intention to commit.

An accused would be guilty of the offence regardless of their motives. To require motive to qualify the intention is fairly restrictive. Motive is a person's reason for conduct. It is something separate and distinct from intention. The general rule is that motive is not taken into account when determining criminal intent.

An accused is culpable where he or she commits a denial of service attack where he or she had the intention to do so. This means that the accused must have had the intent to interfere with access to an information system in such a way as to disrupt services that legitimate users would normally expect to have.

The accused must also have had knowledge of the unlawfulness of his or her conduct. Because the crime requires *mens rea* in the form of intention, liability is now invariably dependent upon the accused having known that he was acting in contravention of the law. It is sufficient that he or she knew, or at least foresaw the possibility, that what he was doing was contrary to law in the broad sense.[122] In other words, the accused must have had known or suspected that he or she

[122] Burchell (n 62) 497, 498 See also S v Hlomza 1987 (1) SA 25 (A) 31, 32

could cause the denial of service. The knowledge component of the intent should be interpreted sufficiently widely to include cases where the accused willfully ignores the unlawfulness of their conduct.

5.3.2 Unlawfulness

The unlawful element of the crime is defined by the absence of permission or authority to interfere with access to an information system so as to constitute a denial of service to legitimate users.[123] The authority must come from the owner or the person lawfully in charge of the information system. The absence of authority is an objectively determinable element. It will be determined with reference to the facts of each particular case.[124]

[123] The authorization may be given so as to test a mail or web sever for example.
[124] Cf. Dicks v South African Mutual Fire and General Insurance Co Ltd 1963 4 SA 501 (N) 504 et seq

Chapter 6

Crimes That Are Not Found in the Electronic Communications Act

The Electronic Communications Act criminalizes some but not all the crimes that can be perpetrated by use of a computer. The crimes of phishing, advance fee fraud, identity theft and cyber stalking are a few of these omitted crimes. The successful prosecution of the persons responsible for these actions will depend upon the official recognition of these conducts as crimes by our law. The object of this portion of the paper is to investigate the possibility of successfully prosecuting the offenders under the common law. Evaluations and recommendations will be put forward in an attempt to shed light on the matters that the legislature should perhaps deal with in the event that the Electronic Communications Act is amended.

6.1 Phishing and Advance Fee Fraud

The activities of phishing and advance fee fraud are not part of the crimes named in the Electronic Communications Act. These offences are discussed below.

6.1.1 Definitions of the Offences

Phishing, also known as carding or spoofing, is characterized by attempts to fraudulently acquire sensitive information such as passwords and credit card

details. The perpetrator masquerades as a trustworthy person or business in an apparently official electronic communication such as an email or an instant message.[125]

Phishing is a form of social engineering. In the field of computer security, social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer commonly uses the telephone or the internet to dupe a person into revealing sensitive information or getting them to do something that is against typical policies. By this method the social engineers exploit the natural tendency of a person to trust another person's word. Phishing does not work by exploiting computer security flaws. Instead, people are perceived as the "weak link" or flaw in computer security and it is this that makes social engineering possible. An example of a social engineering attack is conning a person into believing that the con artist is an administrator and that as an administrator, he or she requests the user's password for various purposes. Users receive messages requesting their passwords and credit card information in order to set up their account, to reactivate settings or some other excuse in what are called phishing attacks.[126] A gullible victim often provides the passwords and other sensitive information to the perpetrator. This grants the individual access to the victim's funds and other property.

[125] http://en.wikipedia.org/wiki/Phishing#Legislative_and_judicial_responses
[126] http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29

Criminal activity that is akin to phishing is advance fee fraud. Advance fee fraud is similar to phishing in the sense that they both rely on the victim being a weak link to computer security. Advance fee fraud is more commonly known as Nigerian money transfer fraud, the Nigerian scam or 419 scams. The modus operandi of a 419 scammer is to pose as the agent of person seeking financial assistance. A typical request reads as follows: "A rich person from the needy country needs to discreetly move money abroad, would it be possible to use your account?" They promise the 'investor' a large portion of the money. A variant of the scam involves a barrister representing the estate of a deceased relative of the victim and claims to have gone to great lengths to find the victim in order to give them their share of the money.[127]

6.1.2 Elements of the Offences

6.1.2 (a) Intention/Culpability

Criminal law recognizes, among others, *dolus directus, dolus indirectus* and *dolus eventualis* as the various types of intention an accused could have when committing a crime. The type of intention required for the crimes of phishing and advance fee fraud is *dolus directus. Dolus directus* is present where the accused's aim and object was to carry out the unlawful act or to cause the consequence even though the chance of its

[127] http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29

resulting was small.[128] The perpetrator need not know the victim personally for a conviction to be secured. The con artists tend to have the direct intention to defraud people regardless of who they are.

An accused is culpable of the offense of phishing and advance fee fraud where he or she had the intention to commit the crimes. The knowledge of the unlawfulness of his or her conduct is a further requirement. Assuming that we had legislation to deal with these crimes, liability for would hinge upon the accused having known that he or she was acting in contravention of the law. The accused need not have known the detailed requirements of the offence charged, the exact section or wording of the legislation or the penalty for the offence, but merely that he or she knew, or at least foresaw the possibility, that what he was doing was contrary to law in the broad sense.[129] In other words, the accused must have known or at least suspected that he or she was acting in contravention of the law.

6.1.2 (b) Unlawfulness

The unlawful element of the crime is defined by the absence of informed consent of the victim to access his or her property. The absence if informed consent or true consent implies or means that there is a lack of permission or authority to access the victim's property.

[128] Burchell and Milton (n 58) 301
[129] Burchell (n 62) 497, 498 See also S v Hlomza 1987 (1) SA 25 (A) 31, 32

6.1.3 Common law

The crimes of phishing and advance fee fraud are not dealt with in any South African legislation let alone the ECT Act. The question that needs to be answered in light of this dearth, is could a conviction ensue against a person caught committing these activities? Two offences in the common law will be briefly discussed to in hopes of identifying a means of securing a conviction. These crimes are housebreaking and theft under false pretences. In addition to this, a statutory initiative taken elsewhere will be looked at to determine whether it could provide some guidance for our legislature.

6.1.3 (a) Housebreaking

Definition

Housebreaking is the crime of unlawfully breaking and entering premises with intent to commit a crime on that premises.[130]

Essential elements of the crime

These are: (1) Unlawful (2) Breaking (3) Entering (4) Premises (5) Intention

[130] Burchell and Milton (n 58) 601

(1) Unlawfulness

The entry of the premises must be unlawful.[131] This means that the person entering the premises must not have a right to do so under some title or contract or because he or she was expressly or impliedly invited.

(2) Breaking

For the crime to be committed there must be a breaking into the premises not merely an entering of the premises.[132] Breaking involves the removal of some obstruction which forms part of the premises. The breaking must involve some displacement of some part of the building. However, breaking may take place without physical damage of any kind.[133]

(3) Entering

To commit the crime the intruder must break into the premises and he must also enter them.[134]

(4) Premises

The general principle is that premises must be 'such as are, or might ordinarily be, used for human habitation or for the storage or housing of

[131] R v Steyn 1946 OPD 426; R v Faison 1952 (2) SA 671 (SR); R v Coetzee 1958 (2) SA 8 (T)
[132] Burchell and Milton (n 58) 603, S v Rudman 1989 (3) SA 368 (E) 385
[133] R v Faison 1952 (2) SA 671 (SR) at 673; R v Willy Ovamboland 1931 SWA 11 in Burchell and Milton (n 58) 60
[134] Burchell and Milton (n 58) 604

property of some kind'.[135] The structure must be a physical one. However, it does not have to be immovable.

It has been held that the following are premises: a store-room, a garage, a shop, a permanently secured tent, an office, an immovable display cabinet separate from but forming an integral portion of a shop, a cabin on board a ship, a small but heavily built concrete mine dynamite magazine and a caravan.[136]

(5) Intention

Intruder must have had the intention to commit a crime on the premises. It is not sufficient that the intruder intended an unlawful breaking and entering.[137]

6.1.3 (a) (i) Evaluation and Recommendations

It is strongly argued that the common law crime of housebreaking cannot apply to phishing scams and advance fee fraud. This is because to perpetrate the crime of housebreaking, the accused must break into the premises of another. The premises must be a physical structure. In order for the crime of housebreaking to apply in this instance the definition of 'premises' would need to be extended to include 'cyberspace'. It is argued that because the courts have limited authority to change

[135] Burchell and Milton (n 58) 604
[136] Burchell and Milton (n 58) 604
[137] Burchell and Milton (n 58) 605

or alter precedent set by previous courts, the recognition of 'cyberspace' as a 'premises' is unlikely to happen soon.

6.1.3 (b) Theft by false pretences

The crime of theft by false pretences is committed by any person who unlawfully and intentionally the steals the property of another. It is carried out by means of misrepresentation of some sort by the perpetrator.[138]

The crime is a cross between theft and fraud. In other words, it has characteristics of both theft and fraud. In theft there must be a taking of another's property. In fraud, there must be a false representation that causes loss to the victim.[139] Our law retains this curious hybrid although the crimes of theft and fraud adequately protect the gullible persons who succumb to the deceit of the tricksters.[140]

Essential elements

The essential elements are (1) Unlawfulness (2) Taking (*contrectatio*) (3) Property (4) Intention (5) Misrepresentation.

[138] Burchell and Milton (n 58) 553
[139] Burchell and Milton (n 58) 553
[140] Burchell and Milton (n 58) 553

(1) Unlawfulness

The taking of the thing must be against the will of its owner. There may be some ground of justification for the taking of another's property for example necessity, statutory authority or consent.[141]

(2) Taking (contrectatio)

Theft is committed by the taking of the property of another person.[142]

(3) Property

Money is capable of being stolen even where it is not corporeal cash but is represented by a credit entry in books of account.[143]

(4) Intention

The fault of theft is intention. This means that the accused must intend to take the property knowing that it belongs to another and that the taking is unlawful.[144] Motive of the doer is irrelevant. The accused must have intended to deprive the owner permanently of 'the whole benefit of his ownership'.[145]

[141] Burchell and Milton (n 58) 543
[142] Burchell and Milton (n 58) 543
[143] Per Holmes JA in S v Graham 1975 (3) SA (A) 576
[144] Burchell and Milton (n 58) 549
[145] Burchell and Milton (n 58) 550 quoting R v Sibiya 1955 (4) SA 247 (A)

(5) Misrepresentation

Misrepresentation is an incorrect statement of fact or law made by one person to another. The misrepresentation may made by words or conduct.[146]

6.1.3 (b) (i) Evaluation and Recommendations

On the face of it, it seems that charging a scammer with theft by false pretences is a surer way of securing a conviction than the charge of breaking and entering. This is because phishing and advance fee fraud both involve the theft of property and the misrepresentation of fact. The misrepresentation typically takes place over the World Wide Web or by means of an electronic message.

California has recently introduced the Anti-Phishing Act of 2005. This Act amends the Federal criminal code and criminalizes internet scams involving fraudulently obtaining personal information (phishing). Snippets of the Anti-Phishing Act of 2005 are as follows:

> *22948.2 It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business.*

[146] Burchell and Milton (n 58) 581

22948.3 (a) The following persons may bring an action against a person who violates or who is in violation of Section 22948.2:

(1) A person who (A) is engaged in the business of providing Internet access service to the public, owns a Web page, or owns a trademark, and (B) is adversely affected by a violation of Section 22948.2

…

(2) An individual who is adversely affected by a violation of Section 22948.2 may bring an action, but only against a person who has directly violated Section 22948.2.

…

(b) The Attorney General or a district attorney may bring an action against a person who violates or who is in violation of Section 22948.2

…

In brief, the Anti-Phishing Act imposes a fine or imprisonment for up five years, or both, on a person who knowingly and with the intention to engage in an activity constituting fraud or identity theft. The accused creates or procures the creation of a website or domain name that represents itself as a legitimate online business without the authority or approval of the registered owner of such business. The accused employs the website or domain name to solicit means of identification from any person.

The Act imposes a fine or imprisonment for up five years, or both, for a person who knowingly and with the intent to engage in an activity constituting fraud or identity theft under Federal or State law. The person must have sent an electronic mail message that falsely represents itself as being sent by a legitimate online business. The person engaged in the illicit activity may have used an internet location tool referring or linking internet users to an online location on the World Wide Web that falsely purporting to belong to or be associated with legitimate business and solicits means of identification from the recipient.[147]

On the face of it, it seems as if section 22948.2 of the Anti-Phishing Act applies in instances where a business was or is being used as a ruse by the person behind the crime. However, certain questions arise with regards to its application. For instance, what is the definition of a 'business' in this context? Does it have to be an existing or legitimate business that is used as a front? Could a person who purports to act as an agent of another person, with no mention of a 'business' in the Web page or the electronic message, be convicted under this Act? The answers to these questions are not entirely clear.

Recommendation

The various conducts which make up phishing and advance fee fraud appear to satisfy the essential elements of theft by false pretences. Be that as it may, it is preferable that the Legislature initiates the criminalization of phishing and

[147] Summary of the Anti-Phishing Act of 2005 available at http://thomas.loc.gov/cgi-bin/bdquery/z?d109:S.472:@@@L&summ2=m&#major%20actions

advance fee fraud. It is suggested that such an initiative will assist law enforcement agencies to secure convictions easily as opposed to attempting to apply the common law to the situation. The legislation, it is hoped, will make the prosecution of the accused less complicated. It is also suggested that the Legislature provide comprehensive definitions and phrase the legislation in such a way that allows the courts to interpret freely. This will assist law enforcement agencies in a world where more and more people are becoming computer savvy and new computer crimes are being created and committed.

A proposal could be made for the inclusion of fault words in any amendment the legislature may make. This is because in construing statutory prohibitions or injunctions the legislature is presumed, in the absence of clear and convincing indications to the contrary, to have intended innocent violations thereof to be punishable.[148] The presence of fault words such as 'maliciously', 'knowingly' or 'corruptly' is somewhat indicative of the legislatures intention to not punish innocent violations of the legislation.

6.2 Identity Theft

6.2.1 Definition of the Offence

[148] As per Botha JA in S v Arenstein 1964 (1) SA 361 (A) 365 This case has been cited in recent judgments: Amalgamated Beverage Industries Natal (Pty) Ltd v Durban City Council (1994 (3) SA 170 (A) SACR 373); Scagell v Attorney-General, Western Cape 1997 (2) SA 368 (CC) (1996 (2) SACR 579); Epstein v Bell 1997 (1) SA 483 (D)

Identity theft or identity fraud is the deliberate assumption of another person's identity. It is usually for economic gain or to frame the person for a crime.

Some people distinguish the terms "identity theft" and "identity fraud". It is said that identity is not something that can be stolen because victims do not cease being who they are. The argument is that the term "identity theft" should apply to unauthorized *access* to personal records and the latter to unauthorized (fraudulent) *use* of such records.[149]

Techniques for obtaining identification range from stealing mail, rummaging through the victim's garbage, stealing personal information in computer databases to the infiltration of organizations that store large amounts of personal information.

Usually, breakdowns in customer privacy, consumer privacy, client confidentiality and political privacy make identity theft possible. In customer privacy situations, it is generally a company that leaked the data in first place. Consumer privacy is violated where credit card numbers or other generally useful identity data are stolen and the information is used much more widely. Client confidentiality and political privacy make it easy to effectively impersonate someone by using confidential information that a person would not ordinarily have access to.[150]

[149] James van Dyke founder of Javelin quoted on http://en.wikipedia.org/wiki/Identity_theft#Objection_to_the_term
[150] http://en.wikipedia.org/wiki/Identity_theft

There are hardships associated with trying to restore the victim's reputation in the community and correcting erroneous information for which the criminal is responsible.

The common law crime of fraud will be examined to determine whether it will suffice to secure a conviction in this regard.

6.2. 2 Elements of the Offence

6.2 (i) Intention

The intention required for the commission of this crime is *dolus directus*.

6.2 (ii) Unlawfulness

The unlawful element of the crime is defined by the fraudulent attempt to impersonate another person.

6.2.3 Common Law

6.2 (a) Fraud

Fraud consists in unlawfully making a misrepresentation which causes actual prejudice or which is potentially prejudicial to another. It is done with the intent to defraud [151]

[151] Burchell and Milton (n 58) 579

Essential Elements of the crime

These are: (1) Unlawful (2) Misrepresentation (3) Prejudice (4) Intention

(1) Unlawfully

Authority, coercion or consent may conceivably remove the taint of illegality from an otherwise fraudulent misrepresentation by a person.[152]

(2) Misrepresentation

Misrepresentation involves the deception or the misleading of the victim of the crime. Misrepresentation is an incorrect statement of fact or law made by one person to another. It may be conveyed in words or conduct. Examples of conduct that is construed as fraudulent conduct include tendering a document or credit card and withdrawing money from an automated teller machine.[153]

(3) Prejudice

The misrepresentation should cause actual prejudice or potential prejudicial to another.[154] The prejudice caused may be proprietary or non-proprietary. Furthermore, potential prejudice suffices.[155]

[152] Burchell and Milton (n 58) 581
[153] Burchell and Milton (n 58) 582
[154] Burchell and Milton (n 58) 579
[155] Burchell and Milton (n 58) 585

(4) Intention

The perpetrator must have intention to defraud and should have intended for statement or conduct to be acted upon. The representations made should have been made knowingly[156] or foreseeing[157] that it might be false.

Buckley J in Re London and Globe Finance Corporation Ltd. states following:

> *"To deceive is to induce a man to believe that a thing is true which is false, and which the person practicing the deceit knows or believes to be false. To defraud is to deprive by deceit; it is by deceit to induce a man to act to his injury. More tersely it may be put that to deceive is by falsehood to induce a state of mind, and to defraud is by deceit to induce a course of action."*[158]

6.2.3 (a) (i) Evaluation and Recommendations

A person found making illicit use of another's personal data could perhaps be charged under section 87 (2) of the ECT Act. It states the following:

[156] Section 245 of the Criminal Procedure Act No. 51 of 1977 assists the State in this regard. It provides that if it is proved that the accused made a false representation, it shall be deemed, unless the contrary is proved, that the accused knew the representation to be false.
[157] See Ex Parte Lebowa Development Corporation Ltd 1989 (3) SA 71 (T) 101–5
[158] Buckley J in Re London and Globe Finance Corporation Ltd [1903] 1 Ch 728 Cf. S v Isaacs 1968 (2) SA 187 (D) 191

A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

It is argued that the courts should consider distinguishing between "identity theft" and "identity fraud". "Identity theft" may be defined as the unauthorized access of the personal records of another. As discussed in the previous chapter of the paper, the words "unauthorized" and "access" would have to be clearly defined. Access to one's records obtained by hacking or by other means such as compiling the personal data of the victim in contravention of section 50 of the ECT Act[159] would be termed "identity theft". The production of "fake data"[160] would include conduct such as switching the perpetrator's name with that of the victim's on his or her identity document for example. The use of that counterfeit identity document would be termed "identity fraud".[161]

A brief appraisal of the common law seems to indicate that a person accused of identity fraud may be prosecuted with a measure of success. This is because the ingredients that make up the crime of fraud are the

[159] Section 50 of the Electronic Communications Act No. 25 of 2002 governs the assembly and use of electronically collected personal information.
[160] Section 87 (2) Electronic Communications Act No. 25 of 2002
[161] James van Dyke founder of Javelin quoted on http://en.wikipedia.org/wiki/Identity_theft#Objection_to_the_term

same or similar to those found in identity theft and identity fraud. These are the elements of unlawfulness, misrepresentation, prejudice and intention.

Perhaps another option could be to use of our current criminal law provision in conjunction with section 50 of the ECT Act. Regardless of this tentative solution, it is nonetheless preferable to have identity theft and identity fraud provisions embodied in a single piece of legislation. A coalescence of the common law and the ECT Act may be too 'messy' for want of a better word. Therefore, it is recommended that South Africa adopt legislation that targets identity theft and identity fraud directly.[162]

On another note, it is questionable whether legal action could be taken against an individual who merely harvested the personal information of another but did not actually use it. It is not certain whether our present criminal law is equipped to handle such a situation. It is put forward that this is one of the situations where the distinction between the terms "identity theft" and "identity fraud" could come into play.

[162] Para 1028 (a) (7) of the Identity Theft and Assumption Deterrence Act 18 USC of 1998 in the United States that targets identity theft specifically. Under this statute, knowing transferring and using without lawful authority a means of identification of another person with intent to commit any unlawful activity constitutes a violation of Federal law or felony. The commission of this crime carries a penalty of up to 15 years imprisonment.

6.3 Cyber stalking

Cyber stalking is a common offence. The Working to Halt Online Abuse organization (WHOA) aims to educate the internet community about online harassment. Comprehensive statistics on cyber stalking are not available. Consequently, in early 2000 WHOA started asking victims for demographic information. The following statistics are based on the cases handled by the WHOA organization where the victims filled out the questionnaire as completely as possible. The figures below are not the total number of cases that the organization handled each year. These figures are as follows:

196 cases for the calendar year 2004

198 cases for the calendar year 2003

218 cases for the calendar year 2002

256 cases for the calendar year 2001

353 cases for the calendar year 2000[163]

This part of the research paper attempts to make out a case for the criminalization of cyber stalking in South Africa. Reference to the common law will be made and an evaluation and recommendations will then follow.

[163] Online harassment or cyber stalking statistics available at http://www.haltabuse.org/resources/stats/index.shtml

6.3.1 Definition of the Offence

Cyber stalking is the use of the internet or other electronic means to stalk someone. This term is also known as online harassment and online abuse.[164]

A cyber stalker does not present a direct physical threat to the victim. They characteristically target and harass their victims via websites, chat rooms, discussion forums, open publishing websites and email. However, the stalker does follow the victim's online activity to gather information and to make threats or other forms of verbal intimidation by electronic means. The anonymity of online interaction reduces the chance of identifying the culprit. [165]

On the surface, cyber stalking might seem relatively harmless. However, it interferes with the individual's privacy, emotional or psychological security and the freedom from being subjected to the control, coercion or intimidation of the stalker so as to be compelled to act in a manner inconsistent with the victim's interests or desires.[166]

[164] http://en.wikipedia.org/wiki/Cyberstalking
[165] http://en.wikipedia.org/wiki/Cyberstalking
[166] South African Law Commission paper on Stalking (Project 130) Issue Paper 22 (2003) available at http://www.law.wits.ac.za/salc/issue/ip22.pdf

6.3.2 Elements of the Offence

6.3.2 (i) Intention

An accused should be found guilty of this offence where he or she directly intended to harass another person. Willful blindness to the possibility of causing fear or anxiety to another person should also be taken into account.

6.3.2 (ii) Unlawfulness

It is suggested that the unlawfulness of the crime may be characterized by the intention to harass or stalk the victim.

6.3.3 Common Law

The main problem is that South African criminal law does not seem to recognize stalking, let alone cyber stalking, as a crime in its own right. Existing criminal law focuses on the punishment of specific prohibited acts. Stalkers may engage in behaviour which is seemingly harmless and lawful when viewed in isolation.[167] It is only where an aspect of stalking behaviour constitutes a criminal act that criminal law may be invoked to restrain or to punish the stalker. Criminal law therefore treats stalking as a precursor to a crime or as evidence of its *mens rea* but unfortunately not as a crime on its own.[168]

[167] Law Reform Commission of Hong Kong Report *Stalking* (2000) 7
[168] South African Law Commission(n 166)

The South African Law Commission looked into the issue of stalking in an issue paper released in 2003.[169] It examined the crimes of common assault, assault with intent to do grievous bodily harm, *crimen injuria*, defamation, malicious injury to property, trespass to land to see whether an alleged stalker could be charged under any of these crimes. After an evaluation of the criminal law, the South African Law Commission concluded that traditional criminal law is inadequate. Prosecuting a stalker for trespassing, for example, will not necessarily provide a remedy unless the stalker enters the victim's private property.[170] Therefore, not much can be done to deter or to punish a stalker until he or she actually causes direct harm to a person or their property.[171] In a bid to assist the victim, the police usually focus upon a particular aspect of the stalker's conduct and seek to bring it within an existing provision of the criminal law. In short, existing criminal law covers some aspects of stalking behaviour. However, legislation is required so as to address stalking as well as cyber stalking as an independent phenomenon.[172]

6.3.3 (i) Recommendations

On the surface, cyber stalking might seem relatively harmless but it can cause victims psychological and emotional harm, and occasionally leads to actual stalking.[173] The United States, Australian and the United Kingdom have enacted legislation targeting stalking. Seeing as our criminal law is insufficient, it is

[169] South African Law Commission (n 166)
[170] South African Law Commission (n 166)
[171] Clark and Van der 'Walt Stalking: Do We Need a Statute?' (1998) 115 SALJ 729 at 731
[172] South African Law Commission (n 166)
[173] http://en.wikipedia.org/wiki/Cyberstalking

suggested that South Africa follow suit and criminalize stalking that takes place by electronic means such as the internet.

Definitions are central to any piece of legislation. However, any definition put forward in the cyber stalking legislation should take into account the unique nature of interaction on the internet. The legislature should perhaps consider whether one's email box qualifies as 'private property' per se. It is recommended that the legislature could define "premises" or the "vicinity" of an individual to include an email address.

Intimidation should be defined as conduct amounting to harassment, repeated and unwanted or unsolicited electronic messages. The messages may be conveyed on a website or blog which the victim is known to frequent.[174] It should be a requirement that the culprit had the intention to cause fear of harm or should have known that their conduct would cause fear. It is put forward that *dolus directus* or *dolus indirectus* should be the standard of intention the courts could use. The motive of the individual would be irrelevant as with other crimes.

It is suggested that the relationship between stalking and sending spam makes for a fairly interesting topic of discussion. The question is whether sending unsolicited bulk (UBE) email to someone could qualify as stalking. The ECT Act criminalizes the

[174] There may be some difficulty with this aspect of the definition seeing as websites and blogs are open to the public.

sending of unsolicited commercial email (UCE).[175] However, there is no mention of unsolicited bulk email or the criminalization thereof. This raises the question of what legal recourse a person could have in a situation where they are the recipient of several unwelcome electronic messages.

6.4 Summary

To sum up, the ECT Act does not criminalize certain undesirable conduct that takes place by electronic means. The ECT Act needs to address the issues of phishing, advance fee fraud, identity theft, identity fraud and cyber stalking directly. It is hoped that this section of the paper illustrated this point. In most instances, our current criminal law cannot adequately cover the offences that are taking place. This makes the prosecution of an accused particularly difficult.

[175] Section 45 Electronic Communications Act No. 25 of 2002

Chapter 7

Conclusion

An evaluation of the common law by the South African Law Commission illustrated that traditional criminal law is inadequate to deal with electronic crime. Section 86 of the Electronic Communications Act represents a fair attempt at criminalizing certain undesirable conduct that may be perpetrated by means of a computer. In the past, organized criminal syndicates targeted governments, businesses and home computer owners alike. The criminal law provisions signify the Legislature's intention to bring these offenders to justice. However, as with almost any new piece of legislation, interpretation problems arise. It has been argued that the Legislature did not provide sufficient and in some cases, any guidance on the interpretation of certain words and phrases. Where this was the case, possible recommendations were made to aide with this problem. Assuming that the Legislature does not rectify the situation by clarifying the meaning of certain terms, it is probable that the courts will be tasked with coming up with appropriate definitions to fill in the gaps.

Lastly, the Electronic Communications Act criminalizes some but not all the crimes that can be perpetrated by use of a computer. The crimes of phishing, advance fee fraud, identity theft and cyber stalking are a few of these crimes that were not included in the legislation. With our law as it stands, the extradition of a person accused of these activities may not be possible. This is because the successful prosecution of such an

accused can only take place if the crime is recognized in the country where the perpetrator or culprit is residing and in the country where he is accused of committing the crime. An examination of the common law shows that trying to secure the conviction of a person accused of these activities will be especially difficult. The deficit in our law can be remedied by an amendment of the ECT Act or by the creation of a new statute. Any amendments to the ECT Act should take into account the peculiarity of internet related activities. It is recommended that the legislature take the initiative and make up for the shortfall in the criminal law provisions of the current Electronic Communications Act. Alternatively, redefining and defining certain things could bring the objectionable conduct under the ambit of the legislation.

Bibliography

Books

Buys R (ed.) *Cyberlaw@SA: The Law of the Internet in South Africa* (2004)

Burchell J *Principles of Criminal Law* (2004)

Burchell J and Milton J *Principles of Criminal Law* (1997)

Harris DJ Cases and Materials on International Law Ships (2004)

The New Shorter Oxford English Dictionary (1993)

Van der Merwe 'Computers' Law of South Africa vol. 5, Part 3 (1998)

South African Law Commission Reports

South African Law Commission *Computer Related Crime: Preliminary Proposals For Reform In Respect of Unauthorized Access to Computers, Unauthorized Modification of Computer Data and Software Applications and Related Procedural Aspects* (Project 108) Discussion Paper 99 (2001)

South African Law Commission *Stalking* (Project 130) Issue Paper 22 (2003)

International Law Commission Report

Law Reform Commission of Hong Kong Report *Stalking* (2000)

Journal

Clark and Van der 'Walt Stalking: Do We Need a Statute?' (1998) 115 SALJ

Articles

Anslie J 'Distributed Denial of Service: Internet as a War zone' available at http://www.networktimes.co.za/article.asp?pklArticleID=3202&pklIssueID=439&pklCategoryID=211

Leggat H 'Hackers Have a Free Ride in South Africa' available at http://estrategy.co.za/article.asp?pklArticleID=2542&pklIssueID=453&pklCategoryID=131

Matai DK 'Cyberland Security: Organised Crime, Terrorism and the Internet' available at http://www.oii.ox.ac.uk/collaboration/lectures/20050210_matai_speech_v1.0_web.pdf

South African Legislation

Copyright Act 98 of 1978

Criminal Procedure Act No. 51 of 1977

Electronic Communications Act No. 25 of 2002

Immigration Act No. 13 of 2002

Interception and Monitoring Prohibition Act No. 127 of 1992

Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002

South African Constitution Act 108 of 1996

International Legislation

United States' Anti-Phishing Act of 2005

United States' Computer Fraud and Abuse Act 18 USC 1030

United States' Digital Millennium Copyright Act

Identity Theft and Assumption Deterrence Act 18 USC of 1998

International Agreements

Additional Protocol to the Convention on Cybercrime (ETS No 189)

Council of Europe's Convention on Cybercrime 23 2001 (ETS No 185)

Guidelines for Security and Information Systems

South African Cases

Amalgamated Beverage Industries Natal (Pty) Ltd v Durban City Council 1994 (3) SA 170 (A)

Cape Town Municipality v Clarensville (Pty) Ltd 1974 (2) SA 138 (C)

Coetzer v Mosenthals Ltd 1963 4 SA 22 (A)

Dicks v South African Mutual Fire and General Insurance Co Ltd 1963 4 SA 501 (N)

Epstein v Bell 1997 (1) SA 483 (D)

Ex Parte Lebowa Development Corporation Ltd 1989 (3) SA 71 (T)

Modderfontein Deep Levels Ltd. And Another v Feinstein 1920 TPD 288

R v Coetzee 1958 (2) SA 8 (T)

R v Faison 1952 (2) SA 671 (SR)

R v Sibiya 1955 (4) SA 247 (A)

R v Silber 1938 T.P.D 561

R v Steyn 1946 OPD 426

S v Arenstein 1964 (1) SA 361 (A)

S v Graham 1975 (3) SA 576 (A)

S v Hlomza 1987 (1) SA 25 (A)

S v Isaacs 1968 (2) SA 187 (D)

S v Nxumalo 1993 (3) SA 456 (O) (1993 (1) SACR 743)

S.A Flour Millers' Mutual Association v Rutowiz Flour Mills Ltd 1938 CPD 199

Scagell v Attorney-General, Western Cape 1997 (2) SA 368 (CC) (1996 (2) SACR 579)

Valkin and Another v Daggafontein Mines Ltd. and Others 1960 (2) SA 507 (W)

International Cases

321 Studios v Metro Goldwyn Mayer Studios Inc 307 F. Supp. 2d 1085

America Online v LCGM Inc. 46 F. Supp. 2d 444 (E.D. Va. 1998)

E.F Cultural Travel BV, 274 F 3d

Fugarino v State 531 S.E. 2d 187 (Ga. Ct. App. 2000)

Re London and Globe Finance Corporation Ltd [1903] 1 Ch 728

Rolls v Miller (1884) 27 Ch.D. 71 (C.A.)

Shaw v Benson, 52 L.J.Q.B 575

Shurgard Storage Centers Inc v Safeguard Self Storage Inc 119 F. Supp. 2d 1121 (W.D. Wash. 2000)

State v Allen 917 P. 2d 848 (Kan. 996)

United States v Morris, 928 F.2d 504, 511 (2d Cir. 1991)

Websites

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

http://www.haltabuse.org/resources/stats/index.shtml

http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

http://www.legal.coe.int/economiccrime/cybercrime/AP_Protocol(2002)5E.pdf

http://news.bbc.co.uk/1/hi/technology/4105007.stm

http://www.oecd.org/dataoecd/27/6/2494779.pdf

http://www.law.wits.ac.za/salc/issue/ip22.pdf

http://www.securitystats.com/infosec.html

www.sophos.com

http://thomas.loc.gov/cgibin/bdquery/z?d109:S.472:@@@L&summ2=m&#major%20actions

http://www.tomwbell.com/writings/FullFared.html

http://en.wikipedia.org/wiki/Cyberstalking

http://en.wikipedia.org/wiki/Digital_Rights_Management

http://en.wikipedia.org/wiki/Identity_theft

http://en.wikipedia.org/wiki/Phishing#Legislative_and_judicial_responses

http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29

http://www.usdoj.gov/criminal/cybercrime/intl/USComments_CyberCom_final.pdf