CHAPTER 11

THEFT

11.1 INTRODUCTION

With the advent of computers and information technology new forms of "theft" emerged. Physical computers and hardware components are no longer the only object of thefts but electronic information, data and software programs are increasingly being misappropriated. Electronic funds can easily be misappropriated through electronic means. Electronic money is often stolen by means of an *electronic funds transfer* which is defined as "a funds transfer effected through the banking system by electronic techniques, with input and output methods being largely or completely in electronic form"[1]. Online banking has created much more possibilities for the cyber criminal to misappropriate funds. Credit or money is often stolen through the *salami* technique.[2] This involves the programming of a computer or software program to round of monetary figures to the nearest rand or cent. The computer or program is then programmed to transfer the smaller amounts to an account controlled by the perpetrator. These small amounts may very soon add up to a substantial amount. It is unlikely that the victims will discover the theft due to the small amounts that are stolen.[3]

---

[1] Ina Meiring *Electronic funds transfers* (1998) Juta's Business Law Vol. 6 Part 1 36.

[2] See Dana van der Merwe *Computers and the law* (2000) 169; A st Q Skeen *Crimes committed by computer* (1984) 14 Businessman's Law 9; A St Q Skeen *Computers & Crime* (1984) 8 SACC 262; Irving J Sloan *The Computer and the Law* (1984) 11.

[3] Van der Merwe (footnote 2 *supra*) 169.

Employees or computer users may "steal" computer time or services. *Data leakage* involves the removal or copying of data from a computer system. Instances of mere copying of data have the outward appearance of theft, but present great difficulties when applied to the ordinary common law principles of the offence. The advent of technology brought us cyber criminals that operate in a digital incorporeal world. The problem however is that the appropriation of electronic data and information places enormous strain on ancient principles that were developed in a tangible and corporeal world.

11.2 THEFT OF INFORMATION

11.2.1 International responses

In the United States of America many States have adopted a haphazard approach to the issue of property. Some States have promulgated legislation that also defines property as inclusive of intangible "property". The Delaware Code for instance contains an offence entitled *theft of computer services.*[4] *Property* is defined as anything of value including data.[5] The State of Illinois provides for a comprehensive definition of *property* in relation to computers and states that property includes electronic impulses; electronically produced data; confidential, copyrighted or proprietary information; private identification codes or numbers which permit access to a computer by authorised computer users or generate billings to consumers for purchase of goods or services. In the

[4] Section 933 of the Delaware Code.

[5] Section 931 (11) of the Delaware Code.

case of *United States v Zinn*[6] the accused gained unauthorised access to computer systems and copied proprietary software.[7] The accused was convicted of some of the charges levelled against him under the United States Criminal Code.[8]

In Canada the theft provision in the Canadian Criminal Code is confined to "anything whether animate or inanimate". It must however be the subject of a proprietary right. In the Canadian case of *R v Stewart*[9] the Ontario Court of Appeal held that theft of information is an offence.[10] The Court found that confidential information is *property* and therefore capable of being the object of theft. The court further stated that information would only be capable of being stolen if it is confidential.[11] This decision was criticised as being too generally formulated, draconian and drastic.[12] However, the Alberta Court of Appeal held in the case of *R v Offley*[13] that information cannot be the subject of theft and did not follow the *Stewart* decision.[14]

---

[6] No. 88 CW – 0673 (N.D. I11 1988).

[7] See Darryl C Wilson *Viewing computer crime: Where does the systems error really exist?* (1991) Computer Law Journal Vol. XI 280 *et seq*.

[8] Wilson (footnote 7 *supra*) 280.

[9] (1983) 42 O.R. (2d) 225; 149 D. L. R. (3d) 583.

[10] See R. Grant Hammond *Theft of information* (1984) The Law Quarterly Review Vol. 100 252 *et seq*.; Grant Hammond *Theft of information* (1988) The Law Quarterly Review Vol. 104 527 *et seq*.

[11] Hammond (footnote 10 *supra*) 258.

[12] See Hammond (footnote 10 *supra*) 258 *et seq*.; Hammond (footnote 10 *supra*) 527 *et seq*.; R G Hammond *The misappropriation of commercial information in the computer age* (1986) The Canadian Bar Review Vol. 64 354 *et seq*.

[13] (1986) 28 C. C. C. (3d) 1.

[14] See Hammond (footnote 10 *supra*) 527 *et seq*. for a discussion of this case.

In the United Kingdom the Law Commission did not address the issue of theft of information neither did the Computer Misuse Act[15]. The definition of *property* in the Theft Act[16] does not include intangible information. In the case of *Oxford v Moss*[17] a student copied an examination paper and was prosecuted of theft of information in terms of the provisions of the Theft Act and it was contended that the paper was an *article of value.*[18] The student was acquitted of theft of information under the Theft Act on the basis that information is not included in the definition of *property*.[19] Similarly in the case of *R v Absalon*[20] it was held that data of an oil company, although very valuable, did not constitute property.[21]

11.2.2. The South African common law crime of theft with specific reference to theft of information

11.2.2.1 Introduction

One of the most interesting debates in legal history is whether a *contrectatio* of an incorporeal is a crime. Many authors have argued at length and have come to different conclusions. The South African Law Commission did not deal with the question of whether theft of

---

[15] 1990.

[16] 1968.

[17] [1978] 68 Cr App R 183.

[18] Edwards, Savage & Walden(editors) *Information Technology & The Law* (1990) 150.

[19] See Chris Reed *Electronic Finance Law* (1991) 226; Edwards, Savage & Walden (footnote 18 *supra*) 150; Ian J. Lloyd *Information Technology Law* (2000) 256 *et seq*.; David I Bainbridge *Introduction to Computer Law* (2000) 316.

[20] [1979] 68 Cr App R 183.

[21] Lloyd (footnote 19 *supra*) 257.

incorporeal "property" should be criminalised, neither is there any provision dealing with this issue in the Electronic Communications and Transactions Act. It is clear that our legislator is silent on the issue and it may be argued that they have decided to leave this aspect over to the judiciary. If not, a suitable provision would have been included in the Act. It will be argued that a proper analysis of the law will lead to the conclusion that theft of incorporeal "property" has indeed been recognised by our law as a criminal offence. The main issue is that it is not property as such and cannot be classified as property within the realm of the law of things. South African courts may be faced with practical difficulties and the judiciary may be hesitant to find that theft of incorporeal "property" is an offence. The reporting and prosecution of such cases will be necessary to develop the law in this regard.

Snyman defines theft as:

> "A person commits theft if he unlawfully and intentionally appropriates movable, corporeal property[22] which
> (a) belongs to, and is in the possession of, another
> (b) belongs to another but is in the perpetrator's own possession; or
> (c) belongs to the perpetrator but is in another's possession and such other person has a right to possess it which legally prevails against the perpetrator's own right of possession
> provided that the intention to appropriate the property includes an intention permanently to deprive the person entitled to the possession of the property, of such property".[23]

[22] My underlining.

[23] Snyman *Criminal Law* (2002) 469. Hunt *South African Criminal Law and Procedure* (1970) on page 566 defines theft as "…an unlawful *contrectatio* with intent to steal of a thing capable of being stolen".

The elements of theft consists of:

1) an act of appropriation;
2) a certain type of property;
3) unlawfulness;
4) intention, including an intention to appropriate.

These elements will be discussed in light of the advent of cyber crime and information technology and specific reference will be made to the possibility of theft of information or data.

11.2.2.2 Appropriation[24]

The *actus reus* required for theft in Roman and Roman-Dutch law was *contrectatio*.[25] The term *contrectatio* referred to the physical handling of the property.[26] It is clear however that our courts have moved away from the requirement that the property need to be physically touched or handled or physically removed from the control of the owner.[27] Some authors are of the view that *contrectatio* is an old and rigid principle which has no place in a modern society.[28] Snyman advocates the approach that the term *appropriation* is more appropriate to describe the act of theft.[29] In the case of *S v Tau*[30] the court followed the appropriation

---

[24] In general see A st Q Skeen *Computers & Crime* (1984) 8 SACC 263 *et seq*.; B J Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 433.

[25] M M Loubser *The Theft of Money in South African Law* (1978) 58 *et seq*.; Hunt (footnote 23 *supra*) 561 – 563.

[26] M M Loubser (footnote 25 *supra*) 58.

[27] M M Loubser (footnote 25 *supra*) 58 *et seq*.; G J Ebersöhn *A common law perspective on computer-related crimes (1)* (2004) 67 THRHR No. 1 28; *S v Naryan* 1998 (2) SACR 345 (W) at 355 *et seq*.

[28] C R Snyman *Nuwe lig op die handelingsvereiste by diefstal* (1998) TSAR 124.

[29] Snyman *Criminal Law* (2002) 476; Also see Snyman (footnote 28 *supra*) 124. M M Loubser holds the same view in *The Theft of Money in South African Law* (1977) 59.

[30] 1996 (2) SACR 97 (T).

theory. An act of appropriation has two elements in that the thief deprives the lawful owner or possessor of his property and then himself exercises the rights of an owner in respect of the property.[31] This approach does not require that the subject of the theft be physically handled and is more appropriate in instances where electronic data is involved. A problem that arises is when data is merely copied.[32] In these instances the owner has not been deprived of his property since the "original" is still in his possession. It can possibly be argued that the owner has been deprived of his exclusive right to the property. However our jurisprudence has not been developed to that stage and it is doubtful whether mere copying will constitute an act of appropriation.

11.2.2.3 A certain kind of property

There are certain requirements that the property must meet before being capable of being stolen:

1) the property must be movable[33];
2) the property must be corporeal, an independent part of corporeal nature[34];
3) the property must be *in commercio*, therefore capable of being sold or privately owned[35]; and

---

[31] Snyman *Criminal Law* (2002) 477.

[32] See M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)* (2003) 1 TSAR 59 – 60.

[33] A person cannot steal a piece of land which is immovable.

[34] Snyman *Criminal Law* (2002) 479.

[35] *Res communes* like the water in the ocean is not capable of being stolen.

4) the property in principle must belong to someone else[36].[37]

Computers and computer components[38] are stolen daily and the common law principles of theft are suitably applicable in those instances. Computers and their physical components are movable, corporeal property that are *in commercio* and can easily be appropriated. However, information, data and software programs are very valuable and yet they are not legally recognised as *property*.

In principle it is argued that only corporeal property can be the object of theft.[39] In the case of *Cheeseborough*[40] the court found that an idea or a design cannot be stolen. Similarly in the case of *Renaud*[41] it became clear that "board and lodging" cannot be stolen. The court recently held in the case of *S v Mintoor*[42] that electricity is not a *thing* and cannot be the object of theft since it is a form of energy and not of a corporeal nature.[43]

---

[36] In principle one can't steal your own property except when the owner steals his own property from someone who has a legally preferent right to his ownership (*furtum possessionis*).

[37] Snyman *Criminal Law* (2002) 479 –181. Also see Hunt (footnote 23 *supra*) 591.

[38] Hardware.

[39] For discussion of these principles in relation to computers see in general J W Dreyer *Computer law in South Africa* (1983) De Rebus 537; D P van der Merwe *Computer Crime* 130 *et seq*.; J P G Eksteen *Die bydrae van akademici tot die regspleging* (1984) Obiter 1; A st Q Skeen *Crimes committed by computer* (1984) 14 Businessman's Law 9 *et seq*.; A St Q Skeen (footnote 24 *supra*) 262 *et seq*.; D J le Roux *Diefstal deur middel van die rekenaar* (1985) August De Rebus 401 *et seq*.; G Horwitz *Computer abuse – the legal implications* (1986) October De Rebus 505 *et seq*.; F R Malan *Oor inligting, rekenaarmisbruik en die strafreg* (1989) De Jure 211; Gordon (footnote 24 *supra*) 433; Adv B Gordon *Theft of information* (2002) August Servamus 32 *et seq*.; D van der Merwe *Computer crime – recent national and international developments* (2003) 66 THRHR 31 *et seq*. and G J Ebersöhn *A common law perspective on computer-related crimes (1)* (2004) 67 THRHR No. 1 28 *et seq*.

[40] 1948 (3) SA 756 (T).

[41] 1922 CPD 322.

[42] 1996 (1) SACR 514 (C).

[43] See Snyman *Criminal Law* (2002) 480 and G J Ebersöhn *A common law perspective on computer – related crimes (1)* (2004) 67 THRHR No. 1 30. However, there are statutory provisions that deal with crimes in respect of electricity in the form of the Electricity Act 41 of 1987.

Although this requirement is firmly entrenched in our law there certainly have been *ad hoc* extensions thereto. The specific form of theft, *furtum possessionis*, bears further scrutiny. This form of theft occurs when the owner of property steals his own property from the possession of a person that has a legally preferent right in respect of the property. According to Snyman, the possessor's right of detention or retention in respect of the property is actually infringed upon.[44] In other words a right is the true object of the theft and a right is incorporeal in nature. It could therefore certainly be argued that our criminal law recognises theft of an incorporeal right in these types of cases.

The development of our criminal law in respect of the theft of money or credit is an apposite example.[45] In an increasingly cashless society credit plays a very important role. Money in the form of notes and coins present no problem since they are corporeal in nature.[46] However, credit is an abstract incorporeal form of money. The bank is the owner of the money in the bank and the client has a personal right to claim the money from the bank.[47] South African criminal law recognises the theft of money in the form of credit.[48] Where a computer is used to transfer amounts (credit) to the perpetrator's account the perpetrators actions will fall within the ambit of theft. In fact theft by means of *electronic funds transfer (EFT)* is a very common occurrence.

---

[44] Snyman *Criminal Law* (2002) 479-480.

[45] In general see D P van der Merwe *Computer Crime* (1983) Obiter 130 *et seq*.; A N Oelofse *Enkele regsaspekte van ontwikkelings in die bankwese* (1985) Modern Business Law Vol. 7 No. 1 13-14; D P van der Merwe (footnote 71 *infra*) 129 *et seq*.

[46] This statement may be subject to scrutiny. Do our bank notes not render proof of a claim against the Reserve Bank?

[47] Snyman *Criminal Law* (2002) 492.

[48] *S v Graham* 1975 (3) SA (A); *S v Kimmich* 1996 (2) SACR 200 (C).

In *R v Manuel*[49] the court stated that in modern banking systems ownership in specific coins no longer arises.[50] In the case of *R v Milne and Erleigh*[51] the court did not expressly find whether incorporeal items could be the object of theft or stolen. In this case a cheque was the object of the theft and the cheque represents a personal right against the bank for the money that the cheque reflects. The court stated in the case of *R v Sibiya*[52] that one should rather look at the "economic effect" of a fraudulent act rather than concentrating on the "concrete mechanics" with which it was committed.[53] In the case of *R v Scoulides*[54] the court found that in these types of cases an incorporeal sum of money is taken and not specific coins or notes. In *S v Gathercole*[55] the court also referred to the abstract sum of money that is appropriated. In *S v Kotze*[56] it was held that the element of property has undergone a change.[57] Therefore in 1970 after consideration of the case law, Coetzee was of the view that theft of incorporeal property in our law is possible.[58] In fact he was of the view that our courts have recognised the concept of theft of an incorporeal for some time, but without formally stating it.[59] In the case of *S v Graham*[60]

---

[49] 1953 (4) SA 523 (A).

[50] at page 526.

[51] 1951 (1) SA 791 (A).

[52] 1955 (4) SA 247 (A).

[53] at page 261.

[54] 1956 (2) SA 388 (A).

[55] 1964 (1) SA 21 (A).

[56] 1965 (1) SA 118 (A).

[57] at page 123.

[58] J A Coetzee *Diefstal van Onliggaamlike Sake?* (1970) 32 THRHR 373.

[59] Coetzee (footnote 58 *supra*) 373.

[60] 1975 (3) SA 569 (A).

the court found that the incorporeal money that a cheque represents is also stolen when a cheque is stolen. The court affirmed this principle in the case of *S v Visagie*[61].

After a thorough analysis of the relevant cases pertaining to theft of money or credit Loubser[62] concludes that the object of theft in cases of this nature can be defined in one or more of the following ways:

1.) It can be defined as a corporeal thing i.e. bank notes or a negotiable instrument;
2.) It can be defined as a right or a claim in respect of a sum of money or credit in a bank account;
3.) It can be defined as an incorporeal sum of money. Loubser refers to it as "an intrinsic value or purchasing power quantified by expressing it as a sum of monetary units".[63]

In the case of *S v Harper and another*[64] it was held that shares which are incorporeal in nature[65], can be stolen. The court found after an investigation of previous case law that our courts have moved away from the requirement of a physical handling of the object. According to Roman and Roman-Dutch law the item in most instances had to be physically handled in order to constitute theft. This requirement necessitated that the item had to be corporeal in nature in order to be capable of being physically handled. Since our courts have moved away from the physical

---

[61] 1991 (1) SA 177 (A).

[62] M M Loubser *The Theft of Money in South African Law* (1977) 49 – 57.

[63] M M Loubser *The Theft of Money in South African Law* (1977) 56.

[64] 1981 (2) SA 638 (D).

[65] As opposed to share certificates which are corporeal in nature.

handling (*contrectatio*) requirement it would seem that the requirement that the thing has to be corporeal in nature has also fallen away.[66] The decision in *S v Tau*[67] also confirms the theory of appropriation to describe the act of theft. This would strengthen the proposition that *contrectatio* is no longer a requirement and therefore paves the way for the appropriation of incorporeal property.

Recently in the case of *S v Kimmich*[68] the court held that the accused not only appropriated the cheques as corporeal objects but also the proceeds or economic value that the cheque represents (which is incorporeal in nature). The court stated:

> "Although in terms of the Roman-Dutch law only corporeal things are capable of being stolen (see S v Graham (supra at 576E)) our Courts have expanded the concept of theft, in respect of money other than physical notes and coins, and have held that a conviction of theft of an incorporeal in the form of (a) a diminution of a credit balance in a complainant's bank account (see S v Kotze (supra)); and (b) the appropriation of the proceeds of a cheque (see S v Visagie 1991 (1) SA 177 (A); S v Graham (supra at 577B)) is competent in our law. Our Courts furthermore do not appear to have had any difficulty in holding that other incorporeals, such as shares, in contra-distinction to share certificates, are capable of being stolen (see S v Harper …)."[69]

---

[66] A St Q Skeen (footnote 24 *supra*) 264 and Ebersöhn (footnote 43 *supra*) 31.

[67] Footnote 30 *supra*.

[68] 1996 (2) SACR 200 (C).

[69] at page 210.

A deeper analysis of the concept property in the law of things should be embarked on. According to the doctrine of subjective rights[70] the concept *thing* is confined to corporeal movable property.[71] Property rights can only be exercised in respect of *things.*[72] Theft constitutes the infringement of property rights and it was therefore also argued that only corporeal property could be the object of theft.

D P van der Merwe in an article entitled *Diefstal van Onliggaamlike Sake met Spesifieke Verwysing na Rekenaars* suggests two solutions in respect of the *lacunae* that exists in respect of theft of incorporeal "property".[73] The first solution would be for the law of things to include incorporeal "property" in the meaning of "thing" and therefore rendering it capable of being owned or possessed.[74] Kleyn argued that the concept *thing* should be defined as anything whether corporeal or incorporeal in nature and that is of value and use to man and which is regarded to be *in commercio*.[75] This definition would include information in the form of data and software programs. Recently Cloete advocated a more modern and broader approach to the concept thing and recommended that a thing should include corporeal and incorporeal items that is of value and use to man.[76] However, Van der Merwe is of the view that the legislator will not

---

[70] Duard Kleyn *Dogmatiese probleme rakende die rol van onstoflike sake in die sakereg* (1993) De Jure Vol. 1 Issue 26 3 *et seq*.

[71] Kleyn (footnote 70 *supra*) 4; D P van der Merwe *Diefstal van Onliggaamlike Sake met Spesifieke Verwysing na Rekenaars* (1985) 9 SACC 130 *et seq*.

[72] Van der Merwe (footnote 71 *supra*) 130.

[73] Van der Merwe (footnote 71 *supra*) 130.

[74] Van der Merwe (footnote 71 *supra*) 130.

[75] Kleyn (footnote 70 *supra*) 13.

[76] Rian Cloete *Die plek en rol van onstoflike sake in die nuwe Suid-Afrikaanse sakereg: 'n kritiese oorsig* (2003) Obiter Vol. 24 No. 1 65 *et seq* (see page 85).

intervene[77] and that development by our courts may be very slow.[78] It is submitted that the suggested extension of the meaning of the concept "thing" to include incorporeal concepts, is not appropriate.

The second solution suggested by Van der Merwe is for the criminal law to extend the category of things capable of being stolen to include personal rights and immaterial property rights.[79] It is clear that our law recognises the *theft of a personal right*, with reference to the various cases discussed above. Certain immaterial property rights such as copyright, trademarks and patents are recognised concepts in our intellectual property law.[80] These immaterial property rights are incorporeal in nature and with time and development the courts will hopefully consider extending the category of things capable of being stolen to include these rights as well (in the same manner in which personal rights have been recognised). It is submitted that the latter (second) solution suggested by Van der Merwe is more appropriate.

A further question that should be considered is whether all types of information should be protected against acts of appropriation. Information in the form of electronic data may take on various forms. In a free and open society information should be available to all. However valuable commercial information that is the product of hard work and expertise should be protected. Trade secrets and confidential information should be protected against unlawful appropriation. It follows that only

---

[77] The legislator did not intervene with the Electronic Communications and Transactions Act.

[78] Van der Merwe (footnote 71 *supra*) 133.

[79] Van der Merwe (footnote 71 *supra*) 130.

[80] See Kleyn (footnote 70 *supra*)

certain types of information should be protected. In other words a person must have a proprietary right in respect of incorporeal or corporeal property such as information protected by copyright and trademark.

It is clear from the discussion thus far that the theft of credit (and therefore personal rights) is a recognised principle in our law. Since credit represents some form of incorporeal "property" our courts in essence have recognised the theft of incorporeal items. The courts have not expressly stated it as such but with time and development this will soon become a reality. Holmes JA stated in *S v Graham*[81]:

> "However, the Roman Dutch Law is a living system, adaptable to modern conditions."[82]

It is clear that our common law is capable of adapting to a modern and technologically advanced era. The theft of credit has evolved to a form of theft with *sui generis* principles and requirements. The theft of data, information or protected ideas should therefore be recognised in our law with its own unique requirements similar to the theft of credit or money. The protection should be limited to certain types of information. The category of things capable of being stolen should be extended to include personal rights and immaterial property rights. The practical implications are that these types of cases will have to be reported, investigated and prosecuted in order for the courts to develop these principles. The accused could raise an objection against the charge sheet on the basis that the charge discloses no offence.[83] Since these are drastic decisions and

---

[81] 1975 (3) SA 569 A on page 576.

[82] See Eksteen (footnote 39 *supra*) 4.

[83] In terms of section 85 of the Criminal Procedure Act 51 of 1977.

have vast implications, the courts may be reluctant to develop and extend the scope of application of theft. An accused has the right to a fair trial, which includes the right to be informed with sufficient particularity of the charge to answer it[84] and not to be convicted for an act that was not an offence at the time of commission[85]. These fundamental rights may impair development by the courts. One should also take care not to use the terms *thing* and *property* where incorporeals are involved.[86]

11.2.2.4 Intention to permanently deprive the owner of his property

The perpetrator must act unlawfully and intentionally. Consent by the owner or lawful possessor may be a ground of justification.[87] A further aspect that should be addressed is the requirement that the perpetrator must have the intention to *permanently* deprive the owner of the full benefits of his or her ownership of the property.[88] When data is intercepted it does not reach its destination. It could therefore be argued that in these circumstances the perpetrator has the intention to permanently deprive the owner of the data. If the court, with reference to the cases discussed above[89], is willing to find that data can in fact be the object of theft, then a perpetrator will have appropriated data with the intention to permanently deprive the owner thereof and could possibly be convicted of theft.

---

[84] Section 35(3)(a) of the Constitution of South Africa, Act 108 of 1996.

[85] Section 35(3)(l) of the Constitution of South Africa, Act 108 of 1996.

[86] Charge sheets should be carefully formulated.

[87] Hunt (footnote 23 *supra*) 575.

[88] See Hunt (footnote 23 *supra*) 579 *et seq*.; Le Roux (footnote 39 *supra*) 401 *et seq*.; A St Q Skeen (footnote 39 *supra*) 10; Horwitz (footnote 39 *supra*) 505.

[89] See paragraph 11.3.3.

Unauthorised use or borrowing of property does not amount to theft.[90] When the perpetrator copies information from a computer or disk, the "original" information is still available on the computer or disk and the owner is not permanently deprived of the relevant information.[91] If the cyber criminal copies the data and then deletes the original file, it could certainly be argued that he has the intention to permanently deprive the owner of his proprietary rights in respect of the data. In cases of mere copying it is argued that the value of the data has been diminished and that the owner no longer has the exclusive use of the data.[92] The perpetrator "steals" a copy of the data and not the data itself. Ebersöhn recently argued that in such instances of mere copying, the perpetrator has the intention to *temporarily* deprive the owner of his control over the data.[93] He also states:

> "It is submitted that our courts should give effect to the economic reality and hold that the intention to <u>temporarily</u>[94] deprive the owner of the benefits of his ownership rights (control) by making an electronic copy and the intention to exercise control over the electronic copy suffices for the purposes of theft."[95]

It is submitted however that our courts have expressly held that mere borrowing or use of an item will not constitute theft.[96] The legislator

---

[90] Snyman *Criminal Law* (2002) 490.

[91] A St Q Skeen (footnote 24 *supra*) 265.

[92] See Adv B Gordon *Theft of Information* (2002) August Servamus 33.

[93] Ebersöhn (footnote 43 *supra*) 38

[94] My underlining.

[95] Ebersöhn (footnote 43 *supra*) 38.

[96] *R v Sibiya* 1955 (4) SA 247 (A).

intervened by enacting a *sui generis* statutory offence.[97] The essence of theft is the intent to permanently deprive the owner of his ownership. One cannot change the essence of an offence in an attempt to force certain case scenarios within its scope and ambit of protection. If the courts allow such an amendment to the basic principles, it may result in an unsatisfactory approach that will leave theft and unauthorised use in the same category. Theft and cases of unauthorised use are fundamentally different due to the requirement that a thief must have the intention to permanently deprive the owner of his ownership. It is difficult to imagine that the courts under these circumstances will discard the element of intent to permanently deprive an owner of his property and it is submitted rightly should not do so. The mere copying of data from a computer system will therefore not satisfy this element and will not constitute theft.

11.2.3 Comparison between theft, unauthorised use and copyright

The "theft" of computer services or computer time is better defined as the unauthorised use of a computer. Employees often use company resources such as computers for personal benefit. It is clear that the mere temporary unauthorised use of an item does not amount to theft.[98] The mere copying of data or information will not amount to theft. Section 1(1) of the General Law Amendment Act[99] provides:

> "Any person who, without a *bona fide* claim of right and without the consent of the owner or the person having control thereof, <u>removes any</u>

[97] Section 1(1) of the General Law Amendment Act 50 of 1956. Also see paragraph 10.4 *infra*. Also compare this with the statutory offence created when a person uses the motor vehicle of the owner without his consent. In this case the owner is also temporarily deprived of his ownership.

[98] Snyman *Criminal Law* (2002) 490.

[99] Act 50 of 1956.

> property from the control of the owner[100] or such person with intent to use it for his own purposes without the consent of the owner or any other person competent to give such consent, whether or not he intends throughout to return the property to the owner or person from whose control he removes it, shall, unless it is proved that such person, at the time of the removal, had reasonable grounds for believing that the owner or such other person would have consented to such use if he had known about it, be guilty of an offence and the court convicting him may impose upon him any penalty which may lawfully be imposed for theft."[101]

The application of this section to cyber offences is somewhat limited due to the requirement that *property* should be *removed from the control of the owner* without consent. The term *property* is limited to corporeal items. Hunt is of the view that the property must be capable of being stolen.[102] The use of the computer itself can be classified as corporeal property. One can argue that the physical computer is used without the consent of the owner thereof. However what is really used is services or time. These are aspects of an incorporeal nature and cannot be classified as property. It could possibly be argued that our courts has now recognised property capable of being stolen to include incorporeal items. Statutes must be interpreted strictly and the court cannot extend the meaning of property within a statute. In our example of information that is copied the perpetrator "steals" a copy of the information. It may be argued that he uses the information without the owner's consent. However the Act expressly provides that *property* must be used without

---

[100] My underlining.

[101] In general see Snyman *Criminal Law* (1995) 473; Hunt (footnote 23 *supra*) 617 *et seq*. Also see Snyman *Die Gemeenregtelike Vermoensmisdade en die Eise van ons Moderne Samelewing* (1977) SACC Vol. 1 18 *et seq* for criticism in respect of this provision.

[102] Hunt (footnote 23 *supra*) 618. Also see A St Q Skeen (footnote 24 *supra*) 266.

the owner's consent. A further problem is the requirement that the property should be removed from the control of the owner.[103] When data is copied it is not necessarily removed from the control of the owner.[104]

A further possibility is to establish whether the data is protected by copyright and whether the criminal's actions do not constitute a copyright infringement. Section 11B of the Copyright Act describes in detail the nature of copyright in computer programs. Section 27(1) of the Copyright Act 98 of 1978 provides:

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

An unauthorised *infringing copy* of the original work must exist. Criminal liability in terms of the Act is limited since section 27(1) is directed at the unlawful distribution of such an *infringing copy*.[105] The mere copying of

---

[103] Le Roux (footnote 39 *supra*) 402; A St Q Skeen (footnote 39 *supra*) 10.

[104] A st Q Skeen (footnote 24 *supra*) 266.

[105] See in general O H Dean *Handbook of South African Copyright Law* (2003) Service 11 pages 1-47 to 1-49.

data protected by copyright will not constitute an offence in terms of the Act.

It is submitted that one should evaluate whether the actions of the perpetrator do not fall within the ambit of the offences created in section 86 or 87 of the Electronic Communications and Transactions Act.[106] For example, in order to copy the data the perpetrator has to secure access to the data, which access could have been unauthorised.[107] In order to obtain the information a data message could have been intercepted.[108] The interception of data is extensively dealt with in the Electronic Communications and Transactions Act and the new "Interception" Act. These actions have the appearance of theft since the sender or recipient is actually deprived of the data. The copying of the data could have caused an unauthorised modification.[109] It should be noted however that the mere copying of data will not constitute a modification. An authorised user may unlawfully copy data. The perpetrator is authorised to access the system.[110] This may constitute a contravention of section 86(1) of the Act if the court can find that the authorised user exceeded the scope and ambit of his authority.[111] A perpetrator may however copy data without specifically gaining unauthorised access to the data.

---

[106] Also see Adv B Gordon *Theft of information* (2002) August Servamus 33.

[107] An offence in terms of section 86(1) of Act 25 of 2002. See chapter 3 *supra*.

[108] An offence in terms of section 86(1) of Act 25 of 2002. See chapter 6 *supra*.

[109] An offence in terms of section 86(2) of Act 25 of 2002. See chapter 4 *supra*.

[110] Some may argue that the perpetrator exceeds the limit of his authority.

[111] See discussion in paragraph 3.7.2 *supra*.

For those instances that cannot be brought under any of the offences as discussed above, it is submitted that there still exists a *lacuna* in our law as far as certain copying offences or unauthorised use offences are concerned. It is recommended that the legislator should intervene and enact a provision in respect of the intentional and unlawful use or copying of data and certain information without authority. The following text is suggested:

> A person who intentionally and without authority copies or uses protected data, is guilty of an offence.

The copying or unauthorised use of data will therefore be criminalised. The data must be electronic in nature and must be protected data. Protected data can then be defined as data in relation to which a person or legal entity has certain proprietary rights such as immaterial property rights.

11.3 IDENTITY THEFT[112]

11.3.1 South African position regarding identity theft

In a technologically advanced era persons can identify themselves through various means including identity numbers, credit card numbers and other account details. This has triggered the phenomenon of identity theft which entails the theft of a person's identity that is subsequently used to impersonate the victim for criminal actions such as fraud.[113] For

---

[112] See in general Murdoch Watney *Identity theft – The dangerous imposter* (July 2004) De Rebus 20 *et seq*. and Benjamin Wright *Internet break-ins: new legal liability* (2004) The Computer Law and Security Report Vol. 20 No. 3 171 *et seq*.

[113] Watney (footnote 112 *supra*) 21.

example a victim's credit card information is "stolen" through means of an electronic card reader or so-called skimming device and used to clone or forge the victim's credit card (which is subsequently fraudulently presented at merchants to effect payment for purchases). The account information is electronic and therefore incorporeal in nature and can traditionally not be the object of theft. Identity theft as such is not *per se* a criminal offence in our law. A perpetrator can however be prosecuted for various other offences such as contravening section 86 of the Electronic Communications and Transactions Act. In our example the perpetrator gained unauthorised access to the data contained in the magnetic strip of the victim's credit card[114] and used a skimming device to overcome the security measures in place to protect the data[115]. The perpetrator can also be prosecuted for fraud in respect of the fraudulent transactions that were conducted with the clone credit card.

11.3.2 International responses

In the Unites States of America identity theft is a crime under federal law as well as certain state laws.[116] The Identity Theft and Assumption Act of 1998 inserted section 1028(a)(7) in the Federal Code. It criminalises identity theft and provides as follows:

> "Whoever knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit or

[114] An offence in terms of section 86(1) of the ECT Act.

[115] An offence in terms of section 86(4) of the ECT Act.

[116] Watney (footnote 112 *supra*) 21.

> otherwise promote, carry on, or facilitate any unlawful activity that constitutes a violation of federal law…"[117]

In California the Database Breach Notification Act[118] provides that if personal information that is stored in a government or private organisation's computer has been compromised, the organisation usually has a duty to notify the victim of this breach.[119]

---

[117] Obtained from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html.

[118] 2002.

[119] Wright (footnote 112 *supra*) 172.