CHAPTER 6

UNAUTHORISED INTERCEPTION

6.1 INTRODUCTION

Cyber criminals often obtain valuable information by intercepting and monitoring communications sent via the Internet or other information networks. Electronic mail messages can easily be intercepted by third parties. This enables cyber criminals to obtain bank account numbers, passwords, access codes and various other valuable data. The private key that is used between two parties to encrypt communications and data can easily be intercepted by a third party. *Wire tapping* involves the interception of data by tapping the communication line between two computers through the use of equipment.[1] A *sniffer* is a program that monitors data that are sent via a network. The phenomenon of *packet sniffing*[2] enables a perpetrator to obtain valuable information such as credit card numbers and secret codes. Information that is sent via the Internet is broken up in smaller parts that are called data packets. The data packets are sent one by one via the Internet and are combined by the recipient's computer. These data packets can be intercepted when they travel via the Internet. A copy of the data packet can be made and the packet can be sent to its original destination. The use of satellite and information networks may facilitate the interception of data.

---

[1] See Dana van der Merwe *Computers and the Law* (2000) 169.

[2] Barrie Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 428.

6.2 INTERNATIONAL LEGISLATIVE RESPONSES

The Electronic Communications Privacy Act[3] in the United States of America provides that the unauthorised interception of an electronic communication is an offence.[4] The interception of an electronic mail message being sent across a network will constitute an offence.

In Singapore section 6(1) of the Singapore Computer Misuse Act[5] states:

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

The Singapore Act provides for the unauthorised interception of any function of a computer by means of a device.[7] The Act further stipulates

---

[3] 1986.

[4] Darryl C Wilson *Viewing Computer Crime: Where does the systems error really exist?* (1991) Computer Law Journal Vol. XI 272 *et seq*.

[5] 1993.

[6] My underlining.

[7] Section 6(1)(a) of the Singapore Computer Misuse Act of 1993.

that *any* device used to unlawfully intercept a function of the computer is an offence.[8]

6.3 INTERNATIONAL RESPONSES BY THE COUNCIL OF EUROPE

The Council of Europe's report on computer-related crime recommends that countries should enact legislation to sanction unauthorised interception with a criminal penalty.[9] This provision is aimed at the protection of data whilst it is being transmitted across a network.[10] Unauthorised interception is on a minimum list[11] as opposed to an optional list[12].

The Convention on Cybercrime[13] deals with illegal interception and provides that the signatory countries should criminalise the intentional interception of data without right.[14] It is clear that the interception of data can only occur when data is transmitted or sent from one point to

---

[8] Section 6(1)(c) of the Singapore Computer Misuse Act of 1993.

[9] Council of Europe *Computer-Related Crime Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems* (1990) Strasbourg 53 – 55; Also see Bernard P Zajac Jr *Transborder Data Flow and 1992* (1990-91) 2 The Computer Law and Security Report.

[10] The following text was recommended in the report: "The interception, made without right and by technical means, of communications to, from and within a computer system or network" (Council of Europe Report *supra* 54).

[11] These crimes should be included in new legislation pertaining to computer crimes. See Zajac (footnote 9 *supra*).

[12] It is optional whether these types of computer crime should be included in new legislation pertaining to computer crimes. See Zajac (footnote 9 *supra*).

[13] Convention on Cybercrime, ETS No. 185, Council of Europe, Budapest 2001.

[14] Article 3 of the Convention on Cybercrime.

another.[15] The Explanatory Report to the Convention on Cybercrime refers to interception offences in relation to *electromagnetic emissions* that are emitted by a computer during its operation.[16] Data can be reconstructed from such electromagnetic emissions and the interception of data in such a manner is therefore possible.

6.4 SOUTH AFRICAN RESPONSES

6.4.1 The Interception and Monitoring Prohibition Act

Section 2(1) of the Interception and Monitoring Prohibition Act[17] states:

> "No person shall –
> (a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or
> (b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization."

The term *intercept* was not defined by the Act. If a person intercepts something that is sent from one place to another, he prevents it from reaching it's destination.[18] The term *telecommunications line* is widely defined in the Act and includes "any apparatus, instrument, pole, mast,

---

[15] Explanatory Report to the Convention on Cybercrime (ETS No. 185) 2001, accessible at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[16] Footnote 15 *supra* paragraph 57.

[17] Act 127 of 1992.

[18] Collins *Essential English Dictionary*.

wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with the sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information". This will include communications sent via the Internet and computer networks. It is submitted that if a person intercepts an electronic mail message for instance, it would fall within the ambit of the Act. *Monitor* would include instances where a communication is looked at, listened to or recorded. The difference between *interception* and *monitoring* is that when one intercepts a communication it does not reach it's destination, whilst monitoring a communication is directed at the monitoring and collection of information during the sending thereof and the communication will still reach its destination. According to Gordon *packet sniffing* would in all probability fall within the ambit of monitoring under section 2(1)(b).[19]

6.4.2 The Interception and Monitoring Bill

During 2001 the Interception and Monitoring Bill was published.[20] According to section 1 of the Bill a *communication* will include a communication in the form of *data*. The interception or monitoring of electronic mail will fall within the ambit of the provisions provided for in the Bill. The Bill in essence provides for the same offences envisaged in section 2(1) of the Interception and Monitoring Prohibition Act.[21] The

---

[19] Barrie Gordon *Internet Criminal Law* in Buys(ed) *Cyberlaw @ SA* (2000) 429-430. See M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 1)* (2003) 1 TSAR 65 footnote 60 for criticism in respect of Gordon's viewpoint.

[20] In general see Saber Ahmed Jazbhay *A threat to constitutional values* (2002) January/February De Rebus 11 *et seq*.; Vivienne A Lawack-Davids *The Interception and Monitoring Bill – Is big brother watching?* (2001) Vol. 22 2 Obiter 347 *et seq*.

[21] See section 2(1) of the Interception and Monitoring Bill, 2001.

term *communication* is widely defined and includes the term *data* which will include electronic communications.[22]

6.4.3 The Regulation of Interception of Communications and Provision of Communication-Related Information Act

The Regulation of Interception of Communications and Provision of Communication-Related Information Act[23] was assented to on 30 December 2002. At the time of writing the Act was not yet in operation. The Act will repeal the Interception and Monitoring Prohibition Act 127 of 1992 when it comes into operation.[24] Section 2 of the Act[25] provides that:

> "Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

Section 49(1) of the Act provides that such an intentional and unlawful interception is a criminal offence. The criminal conduct or *actus reus* will consist of the interception of a communication in the course of its occurrence or transmission. A communication includes a direct and an indirect communication and an indirect communication includes a communication in the form of data.[26] The term *intercept* is defined in the

---

[22] Lawack-Davids (footnote 20 *supra*) 348.

[23] Act 70 of 2002.

[24] Section 62(1) of Act 70 of 2002.

[25] Act 70 of 2002.

[26] Section 1 of Act 70 of 2002.

Act and means the acquisition of the contents of any communication so as to make some or all of the contents of the communication available to a person other than the sender or recipient or intended recipient.[27] The unlawful interception of an electronic message sent via a network will fall within the scope of this section. The term *intercept* will include the monitoring of a communication by means of a monitoring device as well as the viewing, examination or inspection of the contents of an indirect communication.[28] The diversion of an indirect communication from its intended destination to any other destination will also fall within the ambit of the term *intercept.*[29] The interception of the communication has to take place during the course of its transmission. The "interception" of data (which may have been sent as a communication at some earlier time) saved on a disk or in the memory of a computer will not constitute an offence under the provisions of this Act. A perpetrator must act unlawfully therefore without authority or consent of the transmitter or receiver. The intention to intercept and knowledge of wrongfulness are also required. Upon conviction of an offence of contravening section 49(1) a perpetrator may be sentenced to a fine not exceeding R 2 000 000 or to imprisonment for a period not exceeding 10 years.[30]

The Act provides for statutory exceptions to the prohibition of the interception of communications. Law enforcement officers may intercept certain communications in certain circumstances. Section 6 of the Act allows a person carrying on a business to intercept communications, in

[27] Section 1 of Act 70 of 2002.

[28] Section 1 of Act 70 of 2002.

[29] Section 1 of Act 70 of 2002.

[30] Section 51(1)(b)(i) of Act 70 of 2002.

the course of transmission, relating to that business or in the course of the carrying on of that business.[31]

6.4.4 The Electronic Communications and Transactions Act

Section 86(1) of the Electronic Communications and Transactions Act provides:

> "Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts[32] any data without authority or permission to do so, is guilty of an offence."

The Act specifically refers to the intentional interception of *data* as opposed to the term *communication* that is used in the Interception Act.[33] The Act does not define the concept *intercept.* However interception of data supposes the movement of the data. One can only intercept data whilst it is in movement or being sent to a destination. If data is intercepted the data does not reach its destination.[34] Data can be intercepted during the flow of data across computer and information networks. Data that is being transported (therefore not necessarily through a communication) may be intercepted. It is submitted that data that are intercepted through the electromagnetic emissions of a computer

---

[31] This section has been the subject of much debate as to whether an employer may intercept the communications of its employees without their consent. See Jan Stemmett *Interception of communications in the workplace* (2003) Society News 7 *et seq*.

[32] My underlining.

[33] Paragraph 5.4.1 *supra*.

[34] M M Watney *Die strafregtelike en prosedurele middele ter bekamping van kubermisdaad (deel 2)* (2003) 2 TSAR 242.

will also fall within the ambit of this offence.[35] The interception must be unauthorised and therefore unlawful. The interception of data in some instances will amount to theft and a perpetrator can be prosecuted of a contravention of this offence[36], rather than a more difficult and not necessarily successful prosecution of theft of the data[37].

Two smart cards through the microprocessor chips embedded in them can exchange data.[38] A transaction between two smart cards is therefore possible. Data, during the exchange of information, can be unlawfully monitored and intercepted. The Electronic Communications and Transactions Act (and possibly the new Interception Act) will therefore apply in such instances.

There is clearly an overlap between the new Interception Act and the Electronic Communications and Transactions Act in respect of unauthorised interception offences. The ECT Act provides for a penalty of a fine or a term of imprisonment not exceeding 12 months.[39] However, the sentences provided for in the ECT Act, is far more lenient than the penalties provided for in the new Interception Act.[40] A prosecutor may be faced with the difficulty to decide in terms of which Act to prosecute the offender. An accused may challenge such a decision on the basis that his right to a fair trial has been infringed upon.

---

[35] See paragraph 6.3 *supra*.

[36] Watney (footnote 34 *supra*) 242.

[37] See chapter 11 *infra*.

[38] W Faul *Die 'smart' kaart – hoe werk dit?* (1989) 1 SA Mercantile Law Journal 382.

[39] Section 89(1) of Act 25 of 2002.

[40] See paragraph 6.4.1 *supra*.