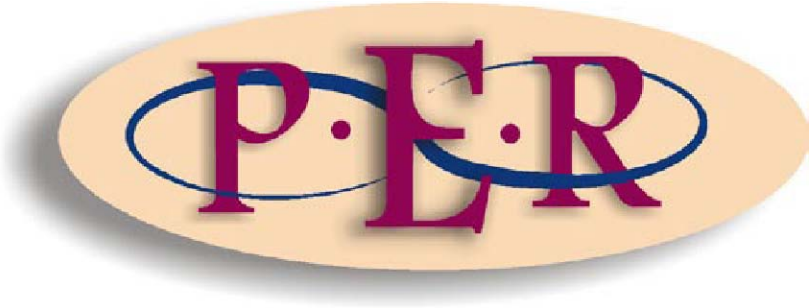
MONITORING, INTERCEPTION AND BIG BOSS IN THE WORKPLACE: IS THE DEVIL IN THE DETAILS?

ISSN 1727-3781



2009 VOLUME 12 NO 1

MONITORING, INTERCEPTION AND BIG BOSS IN THE WORKPLACE: IS THE DEVIL IN THE DETAILS?

T Pistorius*

1 E-workplace: Employers' and employees' perspectives

The introduction of computers into the workplace has significantly changed the way in which employers conduct their business. The rapid deployment and infusion of e-communication technologies in the workplace have affected the way in which employees are expected to perform their duties. These devices have become a standard in modern society and employees are expected to be technologically able.

Technology not only enhances productivity but it also provides an instant, "now" means of socialisation and interaction. Our physical world has become infused with e-communication technologies. Electronic communication paraphernalia, such as multi-functional mobile devices, palm tops and electronic organisers have altered modern communication patterns and social behaviour. E-communication facilities link the office with the home and the home with the office. The border between office and home has become fuzzy as the office is wherever a notebook and a hotspot may be found. This seamless blend of the public and the private raises several difficult legal issues as far as the privacy of e-communications is concerned. The legitimacy of employees' expectations of privacy as far as the use of electronic communication technologies in the workplace is concerned has been debated extensively.[1]

---

* BA (Pret) LLB (Unisa) LLM (Pret) LLD (Pret), Professor of Intellectual Property Law at the University of South Africa. Research for this article has been completed during November 2007."

1 Refer in this regard to the articles by Collier 2002 *ILJ* 1743; Mischke 2001 *Contemporary Labour Law* 91-98; Mischke 2003 *Contemporary Labour Law* 71-80; Van Eck 2001 *De Jure* 364-368; McGregor 2004 *SA Merc LJ* 638-650; Dekker 2004 *SA Merc LJ* 622-637;

When computer equipment was still a novelty in offices, employers adopted a laisser-faire approach to employees' experimental use of these new technologies. Employees were encouraged to become comfortable and familiar with new technologies and to explore the World Wide Web.[2] Two reasons have been cited for this laid-back approach. First, some employers thought that these employees would perform better and secondly, this informal approach was adopted because employers were ignorant of the inherent risk that information technology poses to their businesses.[3]

Employees' expectations to have access to the latest communication technologies and the user privileges that they have become accustomed to, accompany them to the office. Most employees do not give a second thought to the fact that they use the workplace's e-mail facilities also for private purposes. Furthermore, employees have definite expectations that their e-mail communications and surfing habits will be shrouded in a veil of privacy.[4]

The *Constitution of the Republic of South Africa* 1996 guarantees an individual's right to privacy. This right to privacy includes the right of an individual not to have the privacy of her communications infringed.[5] In terms of section 36 of the Constitution all rights may be limited.

The right to privacy in the context of the employment relationship is difficult to define or to elucidate.[6] As noted in the *Moonsamy* case:

> The rights that a citizen is entitled to in his or her personal life cannot simply disappear in his or her professional life as a result of the employer's business necessity. At the same time the employer's business necessity might legitimately

---

Beech 2005 *ILJ* 650-660; Le Roux "Employment" 1-10; Van Jaarsveld 2004 *SA Merc LJ* 651-666; Cohen 2001 *SAJIC* 1-10.

2 See McGregor (n1) 644.

3 *Ibid* 644-645.

4 See *Gouws v Score/Price & Pride Furnishers* 2001 11 BALR 1155 (CCMA); *Philander v CSC Computer Sciences* [2002] 3 BALR 304 (CCMA); *Dauth and Brown v Wier's Cash N Carry* 2002 23 ILJ 1272 (CCMA).

5 See s 14(6) of the *Constitution of the Republic of South Africa* 1996 (the Constitution). See Cohen (n 1) 6-12; Mischke 2003 *Contemporary Labour Law* 72-76.

6 *Moonsamy v The Mailhouse* (1999) 20 ILJ 464 (CCMA) at 469I; Dekker (n 1) 626; McGregor (n1) 639-640.

> impact on the employee's personal rights in a manner not possible outside the workplace. Therefore there is a clear balancing of interests.[7]

In *Protea Technology v Wainer*[8] the court held that a person's right to privacy extends to situations in respect of which a legitimate expectation of privacy could be harboured.[9] However, this subjective expectation of privacy should be viewed as objectively reasonable by society.[10] In the *Protea Technology* case taped telephonic conversations made by the employee relating to the employer's affairs did not enjoy Constitutional protection.[11]

However, employees fail to fully appreciate the overlapping and interrelated rights that are at play here. Viewed from the employer's perspective, it may be argued that privacy is not an absolute right. Employees' right to privacy should be balanced with the employer's business necessities or operational requirements. It should be kept in mind that the employer provides and owns the computer facilities the employee uses. Furthermore, the employer has a right to control the working life of the employee. The employer also has a right to protect her business interests and the integrity of her computing equipment against viruses, excessive use and "cyber loafing", which implies the employee's omission to do assigned work.

It is in this context that Le Roux[12] notes:

> The employer is also permitted to set more general standards relating to conduct in the work place and to the use of equipment and tools. The employer can, for example, prescribe when personal computers may be used, for what purposes they may be used, and how they may be used. The same applies to access to the Internet. If an employee fails to comply with these rules it will, in principle, be open to the employer to discipline an employee for such a failure. In the correct circumstances this may also justify the disciplinary sanction of dismissal.

The *Labour Relations Act*[13] and *Code of Good Practice*[14] place an obligation on the employer to adopt rules or codes of conduct for the workplace that will

---

7 *Moonsamy v The Mailhouse* (1999) 20 ILJ 464 (CCMA) at 471G.
8 *Protea Technology v Wainer* 1997 (9) BCLR 1225 (W).
9 *Ibid* 1239G.
10 *Ibid* 1239G-H.
11 Dekker (n 1) 624-625; *Protea Technology v Wainer* 1240E-F.
12 See Le Roux (n 1) 5.
13 Act 66 of 1995.
14 See sch 8.

create certainty and consistency. Le Roux[15] notes that the rules or codes of conduct must be based on the needs and interests of the business or organisation. The employer also has a right to protect its property and interests and to operate an efficient and effective operation. The employer also has a duty to ensure that the workplace environment is safe and non-discriminatory. These rights and obligations must be weighed up against the rights of an employee.[16] Our courts have upheld rules prohibiting the transmission of sexist and racist messages, or a rule aimed at preventing harassment.[17]

E-communication technology poses several risks to the employers' business. Employees' misuse of e-mail for private purposes may increase the employer's overhead costs, cause communication delays and even blockages of communication systems.

The extent to which an employee's privacy in the work place may be limited by the monitoring of her e-communications is an issue of some complexity and debate.

2 Legislation on interception and monitoring

The question arises to what extent an employer may monitor whether or not employees are using electronic communication technologies responsibly. The answer lies in the interpretation of the *Regulation of Interception of Communications and Provision of Communication-Related Information Act*.[18] The Regulation of Interception Act was assented to on the 30th of December 2002[19] but came into operation only at the end of September 2005.[20]

15 See Le Roux (n 1) 9-10.
16 See Le Roux (n 1) 10; *Bernstein v Bester* 1996 2 SA 751 (CC) 789.
17 See *Bamford v Energiser (SA)* [2001] 12 BALR 1251 (P) and also *Cronje v Toyota Manufacturing* [2001] 3 BALR 213 (CCMA); Le Roux (n 1) 10.
18 Act 70 of 2002 (hereafter the "Regulation of Interception Act" or RICPCIA). Refer to s 2 of Regulation of Interception Act.
19 The Bill was published early in January 2003 – see GN 122 in GG 24286 of 22 January 2003.

Prior to the enactment of the Regulation of Interception Act, the *Interception and Monitoring Prohibition Act*[21] was the most important statutory provision with regard to monitoring. The IMP Act prohibited the interception of confidential information, but the act was not applicable in the private sphere such as the workplace.[22] The reach of the Regulation of Interception Act is wider than that of the previous IMP Act, as the act is also applicable to the private sphere. It prohibits the intentional interception or authorisation of an interception of any communication in the course of its occurrence or transmission. There are, however, certain exceptions, of which some are vital in the context of the employment relationship.

Section 2 of the Regulation of Interception Act constitutes the core provision in this regard. It states that 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.

A contravention of the provisions of the Regulation of Interception Act is a criminal offence[23] with severe penalties.[24]

The term "communication" is defined to include both "direct" and "indirect" communication. The term "direct communication" is of lesser importance for this study as it refers to actual speech or conversation between two persons who are in each other's presence. The definition of "indirect communication" found in section 1 is of greater importance. It reads as follows:

> … the transfer of information, including a message or any part of a message, whether –

---

20 See GN 55 in GG 28075 of 23 September 2005 which proclaimed that the Regulation of Interception Act will come into operation on 30 September 2005 (with the exception of s 40 and s 62 which will only come into operation on 30 November 2005).

21 Act 127 of 1992 (hereinafter referred to as the "IMP Act").

22 See Beech (n 1) 650-654; *Moonsamy v The Mailhouse* (1999) 20 ILJ 464 (CCMA) 467-468. Also refer to Mischke 2001 *Contemporary Labour Law* 92-95. See Cohen (n 1) 3-5.

23 S 49 states that such an action constitutes a criminal offence.

24 In terms of s 51(1)(b) the commission of such an offence could lead to the imposition of a fine not exceeding two million rand or a period of imprisonment not exceeding 10 years.

(a) in the form of –

(i) speech, music or other sounds; data, text, visual images, whether animated or not; signals; or radio frequency spectrum; or

(b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system.

Indirect communication includes telephone calls (land line and cellular); intranet, internet, facsimile facilities, private and personal e-mail messages, tracking devices in company cars; SMS messages and voice-mail messages. The downloading of information from an internet site or the sending or receiving of an e-mail message, or the message itself, would usually fall within the definition of an "indirect communication" as this would, typically, take the form of the transfer of information in the form of data, text or visual images, and it would typically be transmitted by means of a telecommunication system.

The terms "telecommunications system"[25], "telecommunication"[26] and tele-communication facility[27] are defined in section 1 of the *Telecommunications Act*.[28]

The definition of "intercept" is found in section 1. It reads as follows:

> 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 a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the (a) monitoring of any such communication by means of a monitoring device; (b) viewing, examination or inspection of the contents of any indirect communication; and (c) diversion of any indirect communication from its intended destination to any other destination.

---

25 Telecommunication system means "…any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to rearrangement, composition or other processes by any means in the course of their transmission or emission or reception" .

26 The term "telecommunication" means "…the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio or other electromagnetic waves, or any agency of a like nature, whether with or without the aid of tangible conductors".

27 The term "telecommunication facility" includes any wire, cable, antenna, mast or other thing which is or may be used for or in connection with telecommunication.

28 Act 103 of 1996, as amended.

Section 1 defines "to monitor" as to listen to or record communications by means of a monitoring device and "monitoring" has a corresponding meaning. A "monitoring device" is stated to be:

> any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.

An "interception device" is defined as:

> … any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any communication.

The meaning of intercept is important. It includes the acquisition of the contents of any communication through the monitoring of a communication, the viewing of the contents and the diversion of an indirect communication from its intended destination.[29] At the heart of the definition of intercept is the acquisition of the content of the communication and to make all or some of the content available to a person other than the intended recipient or sender. Contents, when used with respect to any communication, include any information concerning the substance, purport or meaning of that communication.

No person may intentionally intercept an e-mail message in occurrence or transmission by using interception or monitoring devices. All activity that monitors the traffic on a telecommunication system is covered by section 2 of the Regulation of Interception Act. To monitor means to record communications, including the mere fact that a communication was sent or a site visited. Indirect communications include furthermore a message or a part thereof in the form of data, text, visual images (text or symbols) in the subject line, text or symbols in filling in recipient's address (223@unisa.ac.za)) and any other form or combination of forms.

29 The blocking or interception of e-mails at server level will thus amount to interception – *contra* Dekker (n 1).

It is also of interest to note that the prohibition in section 2 refers to the interception of a communication "in the course of its occurrence or transmission". This must be read with section 1(2)(a) which states that the interception of a communication takes place in the Republic if, and only if, the interception is effected by conduct within the Republic and the communication is either intercepted, in the case of a direct communication, in the course of its occurrence; or in the case of an indirect communication, in the course of its transmission by means of a postal communication or telecommunications system.

3 Permitted interceptions

3.1 Prior written consent

Sections 3 to 11 of the Regulation of Interception Act set out certain circumstances where there will be no contravention of section 2. Section 4(1) provides for consensual monitoring and states that any person, other than a law enforcement officer, may intercept a communication if that person is a party to that communication. However, of most significance in this context is section 5(1), which provides that any person may intercept any communication if one of the parties to the communication has given prior written consent to such interception. The interception is not legal where it was done for the purposes of committing an offence.[30]

Some have argued that a general consent contained in the conditions of employment of an employee would amount to consent in terms of section 5(1).[31] But the literal interpretation of the wording of this section, namely "consent in writing to such interception" may imply consent on a case-by-case basis. Furthermore, such blanket consent may not suffice as it may be argued

30 See s 5(1).
31 Beech (n 1) 656.

that the employee, when giving the consent, could not have contemplated the scope of the monitoring.[32]

The third important factor to note in the interpretation of section 5(1) is that this consent to monitoring may be given by only one of the parties to the communication. It has been argued that the word "party" in this section bears its ordinary meaning, which would include consent from the recipient, the sender or any party that is copied in the message.[33] In the case of communication between multi-parties, only one party to the communication needs to consent in writing.[34] If proper consent is obtained from the employee this requirement would have been met.

3.2 Carrying on of a business

An important exception is made also for the interception of communications in connection with the carrying on of a business. Section 6(1) states that:

> Any person, may, in the course of the carrying on of any business, intercept any indirect communication (a) by means of which a transaction is entered into in the course of that business; or (b) which otherwise relates to that business; or (c) which otherwise takes place in the course of the carrying on of that business in the course of its transmission over a telecommunications line.

Section 6(2) then sets certain requirements that must be met before the interception of indirect communications in terms of section 6(1) will be permitted. The interception must, firstly, be with the express or implied consent of the "system controller"[35] and the latter, secondly, must either have made all reasonable efforts to inform in advance all persons who intend to use the telecommunication system concerned of the fact that interceptions may take place, or the interception must take place with the express or implied consent of

32 Beech (n 1) 656.

33 Beech (n 1) 656. He also notes that there is a "potential argument" that the employer is a party to the communication because the employer provides the communication equipment, but it is submitted that the employer will not be a "party" to the communication in the ordinary sense of the word.

34 Beech (n 1) 656.

35 The term system controller is defined in s 1. In the case of a juristic person it means the chief executive officer or equivalent officer of the juristic person, or any person duly authorised by such person.

the person who uses the telecommunication system. This telecommunications system must, thirdly, be provided for use "wholly or partly in connection with that business". Such interceptions must, lastly, be carried out for specific purposes, namely, to monitor or keep a record of indirect communications where this is done to establish the existence of certain facts,[36] to investigate or detect the unauthorised use of the telecommunication system concerned; to secure the effective operation of the system or where this is done as an "inherent part of" the effective operation of the system;[37] or to monitor indirect communications made to a confidential voice telephony counselling or support service in certain circumstances.

Section 6 is a tremendously intricate provision. At first blush, it seems that the protection offered by section 6 would apply only to the clients of a business One may also argue that any private use by employees would not fall within the ambit of section 6(1) in that these indirect communications, in the course of being transmitted, would not facilitate the entering into a transaction in the course of the business, would not otherwise relate to the business, or would not otherwise take place in the course of the carrying on of that business.

The aforementioned two statements are open to attack. First, section 6 applies not only to the employer but instead allows "any person" to intercept within the parameters detailed above.[38] Secondly, if it concerned only the employer it could lead to the anomaly that the employer (any person) must obtain consent from the employer (the systems controller) for the intended monitoring. The interception and monitoring of unauthorised use in terms of section 6(2)(bb), thirdly, could include unauthorised communications made from the office equipment of the employer within business hours. One could, however, argue that such unauthorised use relates otherwise to the business, as an employee

36 Beech (n 1) 657-658 notes that this would include the traditional recording of a transaction.
37 According to Beech (n 1) 658 this would include the sending of spam and unusual e-mail traffic to and from a specific user.
38 Note that "any person" is also used in terms of s 5.

of the business makes these communications. Private use will certainly be unauthorised use where the employer's policy or directions say so.[39]

Lastly, doubt has been raised whether or not section 6 is limited to interception in the course of transmission.[40] This last argument maintains that interception may take place in terms of section 6 only if the interception is done whilst the communication is in the process of travelling over internet or intranet. Is it possible to apply this section also to the "interception" of stored messages?[41] Section 1(2)(b) provides that the time during which an indirect transmission is being communicated by means of a telecommunications system includes any time when the telecommunications system by means of which such indirect communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise have access to it. If one considers the definition of telecommunications system set out above, it would appear that the prohibition would extend to the retrieving of communications stored on a mail server.

39 The monitoring or interception by employers of conversations of employees on a private cell phone will not be legal. However, the monitoring and interception of cell phone use will be legal where the employer supplies to the employee the cell phone for use in the business. It will also not cover the tracking of employees' cars (unless the tracking system was provided by the employer for use in connection with business – thus a company car's tracking device).

40 See Buys 2003 www.legalbrief.co.za; Buys 2003 www.estrategy.co.za.

41 The answer is yes. S 1(2) (b) of the Regulation of Interception Act provides that the time during which an indirect communication is being transmitted includes time when the system is used for storing it in a manner that enables the recipient to collect or have access to it. In terms of the IMAP protocol the communication "occurs" only on the shared mail server and while it is there the transmission is incomplete. Where the mail system makes use of the POP protocol the communication will be transferred to the user's computer and deleted from the server.

4 Meeting the requirements of section 5 and section 6 of the Regulation of Interception Act: Introduction to the ECT Act

4.1 Translation of the Regulation of Interception Act to the e-environment

Legal opinion was sharply divided on the implementation of the *Regulation* of Interception Act, specifically regarding the implementation of its sections 5 and 6. The requirement of "written consent" in terms of section 5(1), firstly, posed difficulties.[42] Secondly, the manner in which express or implied consent may be obtained from the system controller or the person who uses the telecommunication system has been questioned. [43] Thirdly, a heated debate centred on the question of what entails "all reasonable efforts to inform in advance" all persons who intend to use the system that interception may take place.[44] Fourthly and lastly, doubt has been raised as to whether or not section 6 is limited to interception in the course of transmission, namely in the process of travelling over the Internet or Intranet. The question has been asked if section 6 could possibly be applied to the "interception" of stored messages.[45]

Other spurious arguments that were raised and which will not be dealt with here were if e-mail filtering and blocking software may be considered illegal[46] and if employment agreements would need to be re-drafted once the RICIPIA becomes effective.[47]

---

42 See s 5(1). See Benn 2003 www.legalbrief.co.za. See Anon 2003 www.legalbrief.co.za.
43 See Benn (n 42) and Anon (n 42).
44 See Sukhraj 2003 www.sundaytimes.co.za.
45 The answer is yes. S 1(2)(b) of RICPCIA provides that the time during which an indirect communication is being transmitted includes time when the system is used for storing it in a manner that enables the recipient to collect or have access to it. In terms of the IMAP protocol the communication "occurs" only on the shared mail server, and while it is there the transmission is incomplete. Where the mail system makes use of the POP protocol the communication will be transferred to the user's computer and deleted from server.
46 See Buys 2003 www.legalbrief.co.za.
47 See Beech (n 1) 658-660; Guedes 2003 www.itweb.co.za.

4.2 Introduction to the ECT Act

It is believed that the *Electronic Communications and Transactions Act*[48] was enacted to remove barriers that previously hampered the validity of electronic consent. The ECT Act aims to remove barriers to the legal recognition of electronic transactions. The ECT Act came into force on the 30th of August 2002. The ECT Act addresses a very wide spectrum of issues covering social, economic and political objectives. This across-the-board approach, of addressing almost all issues related to electronic commerce in one statute, is not common. It has been noted[49] that time will tell whether a piecemeal, *ad hoc* approach or a sweeping pragmatic approach in reforming law is better suited to the logic of electronic commerce. The overall objective of the ECT Act is to enable and facilitate electronic transactions and to create public confidence in electronic transacting.[50]

The ECT Act contains minimalist enabling provisions on contract formation. It seeks to remove legal barriers to e-commerce in South Africa by providing for functional equivalence rules in the electronic contracting context. The ECT Act also seeks to maximise the benefits of e-commerce by promoting universal affordable access to electronic communications and transactions. The ECT Act, importantly, facilitates the legal recognition of data messages by providing that the requirements of writing, signature, and contract formation may be met by such data messages.

Section 1 of the ECT Act provides that a data message means data generated, sent, received or stored by electronic means and includes voice, where the voice is used in an automated transaction[51] and a stored record.[52] "Data" is

48 25 of 2002. Hereafter the ECT Act.

49 See Kaufman and Winn 2000 *ELR* 567-568 who note that the US has followed a piece-meal *ad-hoc* approach, whereas the EU has followed a sweeping, pragmatic approach to law reform in response to technological innovation. Also refer to Pappas 2002 *Denver JILP* 325, 328-331.

50 See s 2(1)(c)-(f), (i)-(o); also refer to Wood-Bodley *SALJ* 526 for comments on the ECT Act.

51 It is unclear why "voice" is confined to automated transactions.

52 The definition of "data message" in the Model Law also refers to "optical" and "digital" means of communication.

defined as electronic representations of information of any kind and electronic communication as a communication by means of data messages. The meaning of the term "electronic" is central to both the meaning of "data" and the meaning of "data message". "Electronic" was defined in the ECT Bill to mean digital or other intangible form. This definition was, however, found inadequate and was deleted from the amended ECT Bill.[53]

Section 3[54] is extremely important in that it confirms that the ECT Act applies to the common law as well as to all existing legislation except where its application is specifically excluded. Section 3 confirms that pre-existing (current) law also apply to the matters outlined in the ECT Act. Party autonomy is retained and whilst the ECT Act merely facilitates e-communications, no-one may insist on the use of an electronic transaction. Entities may furthermore lay down their own requirements, including specific forms, format and standards to be utilised, where they are prepared to use electronic transactions.

4.3 Legal recognition of data messages

Part 1 of Chapter III of the ECT Act provides for the legal recognition of data messages and records. Section 11(1) of the ECT Act provides that information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message. Section 11 embodies the fundamental principle that there should be no disparity of treatment between data messages and paper documents. The form in which certain information is presented or retained cannot be used as the only reason for which that information is denied legal effectiveness, validity or enforceability.

4.4 Incorporation by reference

Section 11(2) also provides that information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to

53 See ECT Bill B8 of 2002 (as amended).

54 S 3 of the ECT Act provides: "This Act must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act".

give rise to such legal force and effect, but is merely referred to in such a data message. The expression "incorporation by reference" is often used as a concise means of describing situations where a document refers generically to provisions which are detailed elsewhere, rather than reproducing them in full.

The objective test of incorporation by reference, as paraphrased in the recent case of *Durban's Water Wonder Land v Botha,*[55] comprises of three elements, namely: first, would the reasonable person have expected terms and conditions of that nature at a resort of that nature? Secondly, were the terms and conditions displayed where one would have reasonably expected them to be displayed, in various languages and in clear and eligible print? Thirdly, were the terms and conditions what may reasonably have been expected, given the nature of the activities?[56]

The translation of these requirements to the on-line world could be – would the reasonable user have expected terms and conditions of that nature as being applicable to that message? Secondly, were the terms and conditions displayed where one would have reasonably expected them to be displayed, in various languages and in clear and eligible print? Thirdly, were the terms and conditions what may reasonably have been expected, given the nature of the activities?

However, new and different standards for incorporation by reference have been created in section 11(3), which could cause confusion. Section 11(3) embodies the common-law approach but adds the requirement that the information to be incorporated needs to be available to the other party online. Uniform resource locators (URLs), which direct the reader to the referenced document, may, for example, be embedded in a message. Such URLs can provide "hypertext links" allowing the reader to use a pointing device (such as a mouse) to select a key word associated with a URL. The referenced text would then be displayed.

55 1999 1 All SA 411 (A).
56 Also refer to Haupt *The pudding is in the proof* 15.

In assessing the accessibility of the referenced text, factors to be considered may include: availability (the hours of operation of the repository and the ease of access); the cost of access; integrity (verification of content, authentication of the sender, and a mechanism for communication error correction); and the extent to which the referenced text is subject to later amendment (notice of updates; notice of policy of amendment). It has been noted that section 11(3) should be abolished, as it increases the common-law burden of incorporation by reference.[57]

4,5 The requirement of a written notice of intended interception and monitoring

The requirement of a written consent or the giving of a written consent may also be communicated electronically. Section 12 of the ECT Act provides that a requirement in law that a document or information must be in writing is met if the document or information is (a) in the form of a data message; and (b) accessible in a manner usable for subsequent reference. This section is intended to define the basic standard to be met by a data message in order to satisfy a requirement that information be retained or presented "in writing" or that it be contained in a "document" or other paper-based instrument.

The information in a data message must be accessible so as to be usable for subsequent reference. Here "usable" includes human and/or computer use and "accessible" is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained.

Section 12 makes reference to the phrase "in law". The precise ambit of this "law" and its scope of application create uncertainty. Following the UNCITRAL Model Law,[58] such a term is likely to be interpreted to refer not only to statutory, regulatory and common law, but also to judicial precedent, procedural and

57 Haupt (n 56) 14-16.

58 See UNCITRAL Model Law on Electronic Commerce 1996 with additional art 5*bis* as adopted in 1998; see also Hill and Walden 1996 www.batnet.com; see Oyarzábal 2004 *U Miami Inter-Am L Rev* 499.

subordinate law.[59] In terms of the wording of section 12 one has to conclude that where parties to an agreement require an amendment of the agreement or a notice in terms of the agreement, that requirement will not be met by a data message.[60] This is problematic. Reference is also made to "law" in other sections of the ECT Act.[61]

4.6 Electronic expression of consent to interception and monitoring

Section 24 of the ECT Act provides that an expression of intent or other statement as between the originator and the addressee of a data message is not without legal force and effect merely on the grounds that—(a) it is in the form of a data message; or (b) it is not evidenced by an electronic signature but by other means from which the person's intent or other statement can be inferred. Section 22 provides for the general rule that contracts can be concluded in electronic form. Section 24 makes provision for the valid expression of the offer and acceptance segments of contract formation as well as unilateral "statements" (subsection (1)). Subsection (2) is designed to include statutory recognition of the click-wrap and web-wrap mechanisms for expressing intent, but is nevertheless open-ended and neutral.

Section 24 is aimed at data messages that relate not to the conclusion of contracts but to the performance of contractual obligations (e.g., notice of defective goods, an offer to pay, and notice of the place where a contract would be performed, recognition of debt). As is the case with section 22, section 24 does not impose the use of electronic means of communication but validates such use. It should not be used as a basis to impose on the addressee the legal consequences of a message, if the use of a non-paper-based method for its transmission comes as a surprise to the addressee. Clearly, where the employer makes use of the electronic environment to convey information to her employees on the use of computer equipment and networks, the use of such a

59 Meiring "Electronic Transactions" 83.

60 Haupt (n 56) 9 argues correctly that an agreement between two parties cannot be elevated to "the law" – it merely has effect in law. S 12 only affects statutory requirements of writing as the common law does not prescribe formality requirements.

61 See, eg, s 12, 13(1), 14(1), 16(1), 17(1), etc.

non-paper-based method for its transmission will not come as a surprise. The use of the electronic environment will rather be viewed as natural and logical.

4.7 Electronic signing

The ECT Act defines an electronic signature as data which is attached to, incorporated in, or logically associated with other data, and which is intended by the user to serve as a signature. Legal recognition is therefore afforded to any method of signing an electronic documents or message, including anything from a password to a scanned "wet" signature.

Section 13(2) provides that an electronic signature is not without legal force and effect merely on the ground that it is in electronic form. Electronic signatures can thus take a variety of forms and, depending on the nature of the transaction, could range between simply writing a name at the end of e-mail to the use of complex biometric-identification technologies. Alongside "advanced electronic signatures" based on public key cryptography, there are various other devices which may currently be used, or considered for future use, with a view to fulfilling in one or more of the functions of a handwritten signature. For example, certain techniques would rely on authentication through a biometric device, where samples of the identifier would have been previously analysed and stored by the biometric device.

Furthermore, section 13(5) of the ECT Act stipulates that any other expression of intent or statement is not without legal force and effect merely on the grounds that—(a) it is in the form of a data message; or (b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred.[62] Parties to a contract may thus agree to use a method other than an electronic signature, to express intent or consent. Electronic agreements may thus be validly concluded through "click wrap agreements" by clicking on the "I agree" icon, or by expressing intent to

62 See s 13(5).

be bound through passwords or any other method from which such intent can be inferred.

5 ECT Act and compliance with the Regulation of Interception Act

5.1 Prior written consent

First, the requirement of prior written consent in terms of section 5(1) will also not pose a problem. In terms of section 12, section 13(5) and section 24(2) of the ECT Act, written consent may be given electronically. The requirement of "prior consent" will be met with ease if the giving of such consent is conditional for obtaining access to the work station or other telecommunication equipment.

5.2 Reasonable steps to inform

Compliance with the requirements of section 6(2) of the RICIPIA, namely, that the systems controller has made all reasonable efforts to inform in advance all persons who intend to use the telecommunications system concerned of the fact that interceptions may take place, will also be facilitated by the ECT Act. It is submitted that it is relatively easy to electronically take reasonable steps to inform.

The ECT Act facilitates this process by affording the employer the opportunity to incorporate her e-mail policy[63] on the welcoming page when employees log on. A clear reference to www.emailpolicy@tana.com will suffice. This notice may be displayed every time an employee logs on to the employer's computer facilities.

63 This should of course contain reference to the monitoring and interception of electronic communications. See McGregor (n1) 647-650 and Van Jaarsveld (n 1) 663-665 for a discussion of the issues to be addressed in the e-mail policy. Also refer to Basset 2003 www.fmew.com.

5.3 Express or implied consent

Compliance with the requirements of section 6(2), namely that the interception must take place with the express or implied consent of the person who uses the telecommunications system, will once again be facilitated with ease by the ECT Act. Incorporation by reference would again prove to be helpful. A standard notice to this effect may also be incorporated in all e-mail messages that are generated or forwarded by the system, which will suffice as notice to third parties.

Obtaining implied consent from the user will be facilitated by sections 11(2) of the ECT Act. The implied consent of a user will be obtained where the employer incorporates her e-mail policy in the welcoming screen of the employee's workstation. A clear reference to www.emailpolicy@tana.com will suffice. This notice may be displayed every time an employee logs on to the employer's computer facilities. The employer may also take one further step to ensure compliance with the Regulation of Interception Act. Users may be required to access a link containing the necessary information prior to obtaining access to the intranet.

Obtaining express consent from the user will be facilitated by sections 11(2), 13(5) and 24(2) of the ECT Act. For express consent users may be required to access a link containing the necessary information and to click that they give consent to such activities by clicking on an icon prior to obtaining access to the intranet or prior to using the workstation.

6 Conclusion

It would seem as though compliance with the Regulation of Interception Act is no Pandora's Box after all. The Regulation of Interception Act's requirements of written consent, taking reasonable steps to inform and obtaining express or implied consent may all be met with ease. The ECT Act's provisions enable employers to integrate these requirements with that of workstation use. It is merely a question of knowing your links and clicks.

Bibliography

Beech 2005 *ILJ*

Beech W "Right of Employer to Monitor Employees' Electronic Mail, Telephone Calls, Internet Usage and other Recordings" 2005 (26) *Industrial Law Journal* 650-660

Cohen 2001 *SAJIC*

Cohen T "'But for the Nicety of Knocking and Requesting a Right of Entry': Surveillance Law and Privacy Rights in South Africa" 2001 (1) *Southern African Journal of Information and Communication* 1-12

Collier 2002 *ILJ*

Collier D "Workplace Privacy in the Cyber Age" 2002 (23) *Industrial Law Journal* 1743-1759

Dekker 2004 *SA Merc LJ*

Dekker A "Vices or Devices: Employee Monitoring in the Workplace" 2004 (16) *SA Mercantile Law Journal* 622-637

Haupt *The pudding is in the proof*

Haupt DM *The pudding is in the proof – Basic principles of the law of contract discussed and applied to instances of 'click-wrap and browse-wrap' agreements* (Unpublished LLM research report Wits 2005)

Kaufman and Winn 2000 *ELR*

Kaufman J and JH Winn "Electronic Promises: Contract Law Reform and E-commerce in a Comparative Perspective" 2000 (27) *European Law Review* 567-588

Le Roux "Employment"

Le Roux PAK "Employment Practices in the Age of the Internet" (Unpublished paper delivered at the E-commerce and Current Commercial Law Workshop on 29 August 2003 at Sandton Johannesburg)

McGregor 2004 *SA Merc LJ*

McGregor M "The Right to Privacy in the Workplace: General Case Law

and Guidelines for Using the Internet and e-Mail" 2004 (16) *SA Mercantile Law Journal* 638-650

Meiring "Electronic Transactions"

Meiring R "Electronic Transactions" in Buys R and Cronjé F (eds) Cyberlaw @ SA II: The Law of the Internet in South Africa 2nd ed (Van Schaik Pretoria 2004)

Mischke 2001 *Contemporary Labour Law*

Mischke C "The Monitoring and Interception of Electronic Communications: Obtaining and Using E-mail and other Electronic Evidence" 2001 (10) *Contemporary Labour Law* 2001 91-98

Mischke 2003 *Contemporary Labour Law*

Mischke C "Workplace Privacy, e-mail interception and the law: Does new Legislation limit employers' Rights to Read E-mail?" 2003 (12) *Contemporary Labour Law* 71-80

Oyarzábal 2004 *U Miami Inter-Am L Rev*

Oyarzábal MJA "International Electronic Contracts A note on Argentine Choice of Law rules" 2004 35 *University of Miami Inter-American Law Review* 499-526

Pappas 2002 *Denver JILP*

Pappas CW "Comparative U.S. and EU Approaches to E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures and Taxation" 2002 (31) *Denver Journal of International Law & Policy* 325-331

Van Eck 2001 *De Jure*

Van Eck BPS "Misuse of Internet at the Workplace" 2001 (34) *De Jure* 364-369

Van Jaarsveld 2004 *SA Merc LJ*

Van Jaarsveld M "Forewarned in Forearmed: Some Thoughts on the Inappropriate Use of Computers in the Workplace" 2004 (16) *SA Mercantile Law Journal* 651-666

Wood-Bodley *SALJ*

Wood-Bowley MC "Wills, Data Messages, and the Electronic Communications and Transactions Act" 2005 *South African Law Journal* 526-528

Register of cases

Bamford v Energiser (SA) Ltd [2001] 12 BALR 1251 (P)

Bernstein v Bester 1996 2 SA 751 (CC)

Cronje v Toyota Manufacturing [2001] 3 BALR 213 (CCMA).

Dauth and Brown v Wier's Cash N Carry 2002 23 ILJ 1272 (CCMA)

Durban's Water Wonder Land v Botha 1999 1 All SA 411 (A)

Goosen v Caroline's Frozen Yogurt Parlour (Pty) Ltd 1995 16 ILJ 396 (IC)

Gouws v Score/Price & Pride Furnishers 2001 11 BALR 1155 (CCMA)

Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA)

Philander v CSC Computer Sciences [2002] 3 BALR 304 (CCMA)

Protea Technology Ltd v Wainer 1997 (9) BCLR 1225 (W)

Register of legislation, official documents and international instruments

Constitution of the Republic of South Africa 1996

Electronic Communication and Transactions Act 25 of 2002

Electronic Communication and Transactions Bill B8 of 2002

GN 122 in GG 24286 of 23 January 2003

GN 55 in GG 28075 of 23 September 2005

Interception and Monitoring Prohibition Act 127 of 1992

Labour Relations Act 66 of 1995

Regulation of Interception of Communications and Provision of Communication-Related Information Act Act 70 of 2002

Telecommunications Act 103 of 1996

UNCITRAL Model Law on Electronic Commerce 1996 GA Res 51/162 of 16 December 1996

Register of Internet sources

Anon 2003 www.legalbrief.co.za

Anon "Office E-Mail: Consent Doesn't have to be in Writing – Expert" www.legalbrief.co.za/view_1.php?artnum=8958 [date of use 5 Aug 2003]

Basset 2003 www.fmew.com

Basset MJ "An Overview of E-mail and Internet Monitoring in the Workplace" www.fmew.com/archive/monitoring/ [date of use 13 Aug 2003]

Benn 2003 www.legalbrief.co.za

Benn W "Written Consent To Intercept E-Mail Is Only One Option For Employers" www.legalbrief.co.za/view_1.php?artnum=9025 [date of use 12 Feb 2003]

Buys 2003 www.legalbrief.co.za

Buys R 2003 The Use Of E-Mail Blocking Software Will Soon Be Illegal In South Africa" www.legalbrief.co.za/view_1.php?artnum=9061 [date of use 5 Aug 2003]

Buys 2003 www.estrategy.co.za

Buys R 2003 Written Consent Or Not: When May Employers Intercept E-Mail? www.estrategy.co.za/article.asp?pk1ArticleIO=2375&pk1IssueID=320&pk1CategoryID [date of use 19 Feb 2003]

Buys 2003 www.legalbrief.co.za

Buys R 2003 E-mail filtering www.legalbrief.co.za/view_1.php?artnum=11156 [date of use 8 May 2003]

Ebersöhn 2003 www.legalbrief.co.za/view_1.php?artnum=9264

Ebersöhn G "The Question of Written Consent" www.legalbrief.co.za/view_1.php?artnum=9264 [date of use 5 Aug 2003]

Guedes 2003 www.itweb.co.za

Guedes G 2003 Legal Loophole Could Make Blocking E-mail Illegal www.itweb.co.za/sections/business/2003/0307161112.asp?O=E [date of use 16 Jul 2003]

Hill and Walden 1996 www.batnet.com

Hill R and Walden I 1996 The Draft UNCITRAL Model Law for Electronic Commerce: Issues and Solutions *The Computer Lawyer* March www.batnet.com/oikoumene/tacr.html [date of use 21 Nov 2004]

Sukhraj 2003 www.sundaytimes.co.za

Sukhraj P 2003 New Law Stops Bosses Spying on E-mail www.sundaytimes.co.za/2003/02/02news/news12.asp [date of use 5 Aug 2003]

List of abbreviations

ch	chapter(s)
ECT	Electronic Communications and Transactions
par	paragraph(s)
reg	regulation(s)
RICPCIA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
s	section(s)
sch	schedule(s)