Monitoring of employee's data messages at the workplace: What about the employee's right to privacy?

Originally publishes in HG.org

http://www.hg.org/article.asp?id=5721

Rationale behind Data Monitoring

The issue of employee's data being monitored by the employer is a contentious issue, which involves the balancing of interests – the employee's right to privacy vis-à-vis the employer's right to remain competitive and efficient. Due to the vast multimedia possibilities created by the internet the employer may be at a potential legal risk as a result of the use and/or conduct of his/her employees whilst using his / her communication tools. Some of the risks associated with this are:

* Leakage of valuable and confidential information
* Vicarious liability of employers – criminal and civil liability (legal liability for employee's action (to be discussed in detail in point 5.))
* Vicarious responsibility for the decimation of child pornography and other unlawful obscene material.
* Decimation of computer viruses
* Loss of productivity and system inefficiency
* Reputation risk due to negative publicity

1. 1. Why Must an Employer Have an Electronic Communication Policy?

In order for an employer to efficiently deal with the aforementioned risk(s) it is essential for the employer to put in place an electronic communication policy as it is not easy to establish whether one's actions are prima facie legally wrongful. The test applied here would be the boni mores test or the reasonableness criteria, which is usually applied ex-post facto (after the occurrence of the incident) and does not help when wanting to "sniff-out" potentially dangerous or offensive electronic content to avoid infringements of the employee's right to privacy.

The question of the employee's right to privacy is an important issue, as the employer must reasonably limit the employees right to privacy by sufficiently monitoring the in- and outflow of data messages. For the purposes of the workplace environment this would entail ensuring that such infringement of privacy would not be tantamount to an acquaintance with personal affairs of the employee. Therefore for the purposes of legal certainty it is essential that an employer put in place such a policy which he/she must strictly monitor and apply.

To assist employers with putting such a policy in place, such a policy must comply with Schedule 8 of the Labor Relations Act (LRA), which contains the Code of Good Practice that states factors that must be applied when disciplining an employee for the contravention of such policy: the employee's awareness of the rule or practice; the reasonableness of such rule or practice; and the consistent application of the rule or practice.

* The employee's awareness of the rule or practice

The LRA's Code of Good Practice places emphasis on the fact that such rules or practices must be clear and unambiguous in order to avoid uncertainty and inconsistency. This has led to the much accepted approach that such a policy must either be expressly contained in ones employment contract or incorporated by reference to which consent has been given. This, however, has not been the view of many Commissions for

Conciliation Mediation and Arbitration (CCMA) case:

- Warren Thomas Griffith vs. VWSA6

The CCMA in this case held that, an employee may be dismissed for willful disobedience, disobeying a lawful instruction and abusing company facilities (unauthorized use of e-mail and Internet). It was the commissioner's view that despite the fact that there had not been any standing rules with regard to the e-mail and Internet use that "… a person with the employee's intelligence and experience …" should appreciate the fact that intentional disregard of the employer's warnings constituted misconduct in the ordinary sense. Furthermore it was stated that an ordinary person understood the meaning of "undesirable" and that pornography would fall within the realm thereof.

* The reasonableness of such rule or practice

In order to establish whether such rule or practice is reasonable or not it will be necessary to investigate whether an employee has the right to privacy at the workplace. There is much doubt whether an employee could raise the defense of infringement of privacy against an employer where he dismisses an employee for sending obscene material using the employer's facilities. Case law supports this view in the following cases:

- Bamford vs. Others vs. Energizer S A Limited

In the said case the employees had been dismissed for repeatedly communicating obscene pornographic material over the workplace intranet. They raised the defense of invasion of privacy but this was turned down by the CCMA as, "… pornographic material consisted purely of material generated by anonymous 3rd parties …" and that such material did not qualify under the right protection.

- Ex parte: Bernstein

Ackerman J., was afforded the opportunity to analyze and discuss the concept of personal privacy and held that "Privacy is acknowledged truly in the personal realm … when a person moves into communal relations and activities such a business … the scope of a persons personal space considerably shrinks". One can draw the inference from the above dictum that when an employee enters the space of business and uses the employers' facilities, a tacit consent to have one's right to privacy is affected.

- Protea Technology vs. Wainer

The court made the following observations, " … The scope of a person's privacy only extends to those issues where the person has a legitimate expectation of privacy … an employee can make and receive calls that are private as long as they have nothing to do with the employer's business … but were it concerns the employers affairs the employer is entitled and may demand a full account … " This rule would obviously also apply to e-mail and Internet use, except where the employee has access to highly confidential information of the company in which circumstances the right to legitimate expectation cannot be catered for.

* The consistent application of rule or practice

In the case of Gouws the CCMA emphasized the application of this rule by ruling in favor of an employee on the basis that the employers had failed

to discipline the employee as to what conduct would be seen as non-permissible and stated that the employer had tacitly waived his right to dismiss the employee as the employee had a reasonable impression that such conduct was not a transgression of any rule.

This however must not be seen as condoning willful improper Internet use – in the case of Bamford, the CCMA dismissed a similar defense as the employee's action indeed constituted conduct, which could result in risk of dismissal. The court held that "... e-mail trafficking of pornography is damaging to the employer … the risk of the employer's domain being exposed to association with such obscene sites … the risk of the employer being vicariously liable…"

2. Data Interception and Monitoring

The Interception and Monitoring Act, the Regulations of Interception of Communications and Provision of Communication Related Act (RICPCRA), the Electronic Transaction Act and the Promotion of Access to Information Act (PROATIA) generally prohibit the unlawful interception or monitoring of any data message.

2. 1. General Prohibition of Data Interception and Monitoring

The Interception and Monitoring Prohibition Act specifically governs the monitoring of transmissions including e-mail. Section 2 states that: no person shall –

"intentionally intercept or attempt to intercept or authorize, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission "

This means in simple terms that conduct that:

(a) Intentionally and without the knowledge or permission of the dispatcher to 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 monitors any conversations or communications by means of a monitoring device so as to gather confidential information concerning any person, body or organization,

is unlawful and therefore prohibited. One must note that the attempt thereof is as sanctionable as the actual act of unlawfully intercepting and monitoring of a data communication. One must however read the provision so as not to exclude any other accepted lawful grounds of justification such as, necessity, private defense, lawful interception, consent, court order or interception directive.

2. 2. Data Interception and Monitoring by Consent

In terms of Section 5 (1) of the RICPCRA provides that any person may authorize or given anyone else the permission to monitor and or intercept any data communication unless such is for the purposes of unlawful conduct. Furthermore the RICPCRA, which authorizes the interception by law enforcement under certain instances as prescribed in subsection (2) (a), (b) and (c). Any conduct outside the scope of section 5 as provided for by

common law would be unlawful unless expressly justifiable under the accepted grounds of justification as mentioned earlier.

2. 3. Data Interception and Monitoring of Indirect Communications at the Workplace

One must note that despite the fact that Section 5 authorizes the data interception of "indirect communications" by consent of the parties engaged in the data communication, Section 2 is also subject to certain exceptions as contained in Section 6 of the RICPCRA expressly allows the direct or indirect interception within the scope of business.

Section 6 states that:

(1) 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;
(b) which otherwise relates to that business; or
(c) which otherwise takes places in the course of the carrying on of that business, in the course of its transmission over a telecommunication system.

(2) A person may only intercept an indirect communication in terms of subsection (1)

(a) if such interception is effected by, or with the express or implied of the, system
controller,
(b) for the purposes of –

(i) Monitoring or keeping record of indirect communications-
(aa) in order to establish the existence of facts,
(bb) for purposes of investigating or detecting the unauthorized use of the
Telecommunications system; or
(cc) where that is undertaken in order to secure, or as an inherent part of the effective operation of the system

(ii) Monitoring indirect communications made to confidential telephony counseling or support service which is free of charge, other than cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they choose to.

Furthermore Section 6 subsection (c) and (d) add further requirements that such interception must take place either partly or wholly on the telecommunication system of that business and that the person being intercepted must have either consented by free will or tacitly by his actions and/or what he / she reasonably ought to have known.

To satisfy these provisions, as stated above, the employer must inform employees that it may read the employee's messages and it should describe under what circumstances it will do so. As stipulated previously an employer could circumvent these provisions by stipulating in the employment contract of policy that "… In the event of a suspected misconduct involving abuse of the internet or e-mail facilities of the employer, the employer reserves the right to monitor suspected employee's e-mail and web…" It must also be stated that the meaning of "indirect communication" must be

given a wide meaning as to include all platforms and/or media available on the different communication networks.

It should also be clear that section 45 read together with Section 45 of the RICPCRA specifically prohibits the use, manufacture, possession and/or advertising of any of the listed items as per Gazette Notice in terms of section 44(1)(a).

It is clear from section 6 that interception of data messages will only be justifiable in certain specific instances mostly related to business and that any deviation from the general rule prohibiting interception would be a violation of privacy and criminally and civilly sanctionable in terms of Section 86 (1), (2) and (3) of the ECT and would result in a fine or imprisonment not exceeding 12 months.

3. The Doctrine of "Vicarious Liability "

The general rule is that the employer is responsible for the wrongful acts of his employee committed in the execution and /or during the course of his employment. This doctrine of law is controversial as it places legal liability on the employer even in instances where the employer could not have reasonably prevented the damage caused such as in the case of offensive, hate, pornographic and abusive e-mails or data communications by his / her employees.

It is a thin line in determining whether the employee was acting in the scope of his employment or in a frolic of his own. Our courts have managed to develop the following test in the case of Boland Bank Bpk vs. Bellville Municipality to bring clarity on the aforesaid issue, the court said:

"In order to determine whether an act was committed in the scope of employment, one must ask whether the act in question was committed whilst busy with an act closely enough related to his employment task."

There are instances when the court refused to hold the employer vicariously liable on policy considerations where the employer engaged in a "frolic of his own" but the line between liability and non-liability is so small and requires that the Employer at least try and cover all possible delictual pitfalls.

It is, however essential, to make a brief overview of the possible liabilities that one might incur as an employer in the cyber-environment.

4. Cyber-porn and Sexual Harassment in Cyberspace?

As already mentioned, the undesirable and unlawful possession, use and/or decimation of pornographic material and/or child pornography at the work place is a punishable offense for which an employer may "summarily dismiss" the employee in question and could be regarded as having procedurally and substantively fairly dismissed the employee in terms of the Labour Relations Act 66 of 1995. It is also law that anyone who contravenes Section 25 and Section 27(1) of the Films and Publications Act 65 of 1996 by decimating or being in possession of child pornography by electronic data communication means is guilty of a criminal offense.

However, this does not end the enquiry as the said offender might have sent the said indecent electronic material to fellow employees or 3rd parties outside the organization and could have seriously offend them exposing the owner of the originating e-mail address to delictual claims for infringement of the employees and/or 3rd party's dignitas and fama. The possibility of an employee "sexually harassing" a fellow employee with the

aid of obscene pornographic electronic material can also not be excluded and could result in the employer being held vicariously liable in a civil action resulting from the alleged act of sexual harassment as the Employer has a duty to ensure and/or put in sufficient measures in place to ensure that sexual harassment does not take place at the workplace.

It is submitted that employers must make use of electronic content filters to regularly filter out suspicious and offensive electronic content to avoid its decimation on the local intra-net and or the larger world wide web via any of the employers' communication devices.

5. Is an E-mail Disclaimer Enough to Offset Vicarious Liability?

The legal position as to the validity and effectiveness of e-mail disclaimer has been and still is a serious problem in many countries of the world including South Africa. It is however interesting to note that although in some jurisdictions it is not referred to as a disclaimer notice but rather as a legal notice. This is primarily due to the fact that the word Disclaimer is misleading as it presupposes that the reader of the e-mail coupled with an e-mail disclaimer consented to the terms merely by having read the said e-mail. It is interesting to note that interesting suggestions have been offered from the different world jurisdictions.

Simon Halberstam, a practicing solicitor at Sprecher Grier Halberstam had the following to say about the effectiveness and validity of e-mail disclaimers, with regards to English law:

"The value of disclaimers is limited, since the courts normally attach more weight to the substantive content of the communication and the circumstances in which it is made than to any disclaimer… disclaimers may possibly be helpful if an issue ends up in court… since disclaimers … Even though their effectiveness in court is doubtful, they may provide a useful argument in negotiations to resolve a dispute."

The question that immediately arises, since the disclaimer is a unilateral act is whether the disclaimer is legally effective. As there is definitely legal uncertainty as to the legal recognition of such disclaimers, Halberstam submits that its efficiency is almost certainly enhanced if any one or both of the following factors are to be considered:

i. "If the disclaimer appears at the top rather than the bottom of the e-mail. In this way, the e-mail comes to the attention of the recipient before he/she has read the contents of the e-mail so that in the same way as a fax front sheet disclaimer, the recipient can make an informed decision whether to proceed to read the contents."

ii. "If the recipient has had previous correspondence with the sender of the e-mail, the recipient may be taken to have digested the contents of previous e-mail disclaimers and it would be reasonable to conclude that he/she received the e-mail with full notice of the standard disclaimer and could have refused to continue the correspondence exchange should he/she have been unwilling to accept the terms of such disclaimer."

iii. "The actual contents of the disclaimer are important. It must cover the various areas of potential liability in such a manner as to satisfy the relevant guidelines which have arisen from recent case law and, also, statute."

In Holland for instance § 3 of the Netherlands Civil Code (BW) states that legally relevant acts can be done by direct communication and or by tacit consent or any other legally relevant act as they have been deemed to have been received as the (BW) favors the "reception theory" which would result in the recognition of e-mail disclaimer solely on the basis that the e-mail is deemed to have been received and read. This however must be balanced with the "cognizance theory", which assumes that after receiving the said information one has the choice to read the e-mail subject to the

limitations or leave it alone. It is interesting to observe that the Netherlands Supreme Court is disposed towards the reception theory.

When looking at the South African situation Reinhardt Buys suggests that, a legal disclaimer could be a legally binding term of an agreement and should rather be referred to as a 'legal notice' instead of the term legal disclaimer. Buys suggests to have the full effectiveness of the disclaimer, one should place the disclaimer and/or the link thereof to be conspicuously visible and must have an " I accept" button (icon) that would constitute the electronic certification of an electronic signature without actually using any marks or form of conventional electronic signature.

Migley is of the view that e-mail disclaimers amount to a contractual exclusion of liability and/or is the basis for the defense volenti non fit injuria (meaning voluntary assumption of risk or consent to risk). Furthermore it is submitted that the terms are valid and binding on the addressee as he/she would have seen the contents of the e-mail and the doctrine of constructive notice or information theory would apply but are used cautiously usually to the advantage of the plaintiff.

In short, since this form of legal disclaimer is still questionable, it is advisable to put in the necessary preventative measure regarding e-mail use and content filtering in order not to run into any legal disputes.

ABOUT THE AUTHOR: Sizwe Snail (LLB) – UP

Sizwe Snail Director at SNAIL ATTORNEY @ LAW

.The article was initially written whilst employed as Attorneys at Couzyn, Hertzog & Horak

More information about Couzyn, Hertzog & Horak

Endnotes:

1. S Snail (2005). Legal aspects of the Internet at the workplace, Unpublished Paper- Presented at University of North West, Department of Management, 12 August 2005

2. D Goodburn and M Ngoye (2004). Privacy and the Internet in R Buys (2004) Cyberlaw @ SA (2nd Edition)

3. Tommie Meyer vs. University of Pretoria

4. S Snail (2005). Legal aspects of the Internet at the workplace, Unpublished Paper- Presented at University of North West, Department of Management, 12 August 2005

5. Act 66 of 1995

6. D Goodburn and M Ngoye (2004). Privacy and the Internet in R Buys (2004) Cyberlaw @ SA (2nd Edition) p.179.

7. Ibid.

8. 2001 12 BALR 1251 (P)

9. 1996 (2) SA 751 (CC)

10. 1997 (9) BCLR 449 (W)

11. (2001) 10 CCMA 8.32.1 case number EC21512

12. D. Goodburn and M. Ngoye (2004). Privacy and the Internet in R Buys (2004) Cyberlaw @ SA (2nd edition) p.182.

13. Supra

14. Act 70 of 2002

15. S Snail (2005). Legal aspects of the Internet at the workplace, Unpublished Paper- Presented at University of North West, Department of Management,12 August 2005

16. In the English case of R. vs. Secretary of State for Home Department, ex-parte Rudduck and others 1987 2 ALL ER 516 were the court warned that the grounds of justification based on common law must be used sparingly and must not be readily available as a defense to the allegation of unlawful interception and monitoring of data communications. The learned judges made mention of the fact that there are provisions authorizing law enforcement officers to intercept and monitor data communication but the procedure for getting search warrants, interdict and/or interception and monitoring directives (as stated in the South African law) they must be strictly adhered to as this could cause an erosion to the individuals right to privacy. Also see section 3 (a) and (b) of the RICPCRA on the provision regarding the execution and issuing of interception directives.

17. This seems to be consistent with the common law approach in English law. In the case of R v Rasool and another 1997 4 ALL ER 439, Lords Stuart – Smith L.J., Forbes and Brian Smedley J.J. came to the conclusion that a communication interception were a "police-trap" had consented o the data interception would be admissible in a Criminal proceeding.

18. S. Snail (2005). Legal aspects of the Internet at the workplace. Unpublished Paper- Presented at University of North West, Department of Management, 12 August 2005

19. This includes any instrument or devices or equipment capable of being used to record and or monitor communication being put in or retrieved from a computer and including but not limited to telephone wiretaps, keystroke recorder, software that has the ability to store and retrieve information without the author, miniature laser transmitters, cellular intercepting devices, miniature sound recording devices and any other not listed device that could be useful in the unlawful intercepting and monitoring of data communications.

20. 1981 2 SA 437 (C) 444-445

21. Bamford vs. Others v Energizer S A Limited 2001 12 BALR 1251 (P)

22. De Reuck vs. Director of Public Prosecutor and Others. 2003 (3) SA 389 W.

23. See the case of Naspers (Media 24) vs. Grobler (Case Summary in "A brief history of judgments and decisions having an effect on or resulting from the use of technology in South Africa 1993 to 2005")

24. H. Snijders (2003). The moment of effectiveness of e-mail notices in H. Snijders and S. Whetherill (eds.). E-commerce Law, p80.

25. Ibid at.p.81.

26. S. Nel (2004). Freedom of expression on the Internet Privacy and the Internet in R. Buys (2004) Cyberlaw @ SA (2nd Edition) p.208.

27. Migley (2001). Cyberspace Issues, in Burns, Communications Law, p.398.

28. S. Snail (2005). Legal aspects of the Internet at the workplace. Unpublished Paper- Presented at University of North West, Department of Management, 12 August 2005