

MANAGING INTERNET & E-MAIL ABUSE

By J Michael Judin & M Shaheem Samsodien
of Goldman Judin Maisels Inc

SCOPE OF THE PROBLEM

Extensive research conducted in the USA¹ shows that there: 97% of companies experience employee abuse of Internet resources; 66% of companies have disciplined employees for Internet abuse, while 33% of companies have dismissed employees; up to 40% of employee Internet usage is non business related; the average loss per company due to employee abuse per annum is some \$100 000, although losses at individual companies are as high as \$3-million; enterprise bandwidth needs doubling every 90 to 180 days; 38% of companies experienced between 1-5 security breaches that originated within the organisation (many of which occurred because employees were unaware of how their computer use impacted on company security); and 80% of companies monitor online behaviour by employees.

Although local research has been more moderately undertaken, an extrapolation of the results of a recent survey of public companies in South Africa² reveals that: 69% experience loafing on the Internet; 70% experience accessing, downloading or sending through e-mail of discriminatory or sexually offensive jokes or pictures; 65% experience clogged bandwidth or degraded system performance through abuse of the Internet system; 6% experience the violation of copyright laws or the posting of information in the name of the company that defames other companies or individuals; 60% have disciplined employees for Internet and e-mail abuse; and 77% have reserved the right to monitor online traffic at any time.

As the full implications of Internet and e-mail abuse have yet to come to the fore in our courts, it is useful to reflect on a

couple of judgments from foreign jurisdictions.

Provident Society v Norwich Union: The British High Court found that Norwich Union had defamed a competitor by sending an e-mail message wrongly suggesting that its competitor was close to insolvency. The message was originally sent on Norwich Union's own internal e-mail system but was inadvertently transmitted to third parties and found its way to the Provident Society who sued for damages. The court found that Norwich Union was responsible for what had been written on the system by its employees and ordered payment of £450 000 as compensation to the Provident Society.³

John Kelley v Airborne Freight Corporation: Kelley was awarded some \$3.2-million by an US court after it was established that his dismissal constituted an act of age discrimination (he was 46 and his replacement 37). What tipped the scales in favour of Kelley were a series of incriminating e-mails exchanged between Kelley's superiors, which had been disclosed as part of a routine process of discovery in preparation for the trial.⁴

US Auto Workers: In this American case a group of Black employees successfully sued their employer for racial harassment. The employees alleged that a hostile working environment had been created by e-mail parodies of African American speech patterns circulated on the internal e-mail system.⁵

Although the problems created by Internet / e-mail abuse are virtually endless, the primary challenges are these: Cyberloafing – loss of efficiency coupled with degradation of system; threats to the security of information; the threat of internal discrimination challenges caused by a hostile working environment –

¹ 1999 Computer Security Institute/FBI Computer Crime and Security Survey as discussed by Robyn Weeda, "The Enemy Within", *People Dynamics* May/June 2001; Samuel Greengard, "The High Cost of Cyberslacking", *Workforce*, December 2000, vol. 79, no. 12, p. 22.

² Lisa Dancaster, "Internet Abuse: A Survey of South African Companies" (2001) 22 *ILJ* 862.

³ Case discussed by Nikki Pennel and Stefan Barrow, "Unlawful Surfing", *People Dynamics* July 2001 at 34.

⁴ Case discussed by Brenda Sunoo, "What if Your E-mail Ends Up in Court?", *Workforce*, July 1998, vol. 77, no. 7, p. 36.

⁵ See fn. 3 above.

discrimination on the grounds of sex, race, religion or culture, etc; the threat of external challenges based on defamation and infringements of copyright; and the threat to business relationships (of all forms) caused by the association of the company domain name with offensive e-mail.

ENERGIZER: A CASE STUDY

In October 2000, Energizer (SA) Limited (the company) dismissed five women for e-mail abuse (the employees). After conciliation had failed, the employees embarked upon an extensive media campaign in an endeavour to clear their names.⁶ A year later, and after two of the employees had abandoned their cases a few days before the commencement of the proceedings, the matter proceeded to private arbitration before Advocate R Sutherland SC (the arbitrator), who ultimately found the dismissal of the remaining three employees both substantively and procedurally fair. Much of the publicity surrounding the *Energizer* case was attributable to the fact that it was the first case in South Africa to deal with a host of thorny issues relating to e-mail abuse, many of which were dealt with by the arbitrator in his lengthy award. *Energizer* thus serves as a useful case study.

- **Factual background**

The employees were employed (in marketing and administration positions) at the company's head office in Woodmead outside of Johannesburg. Although they did not have direct access to the Internet, each of them had access to the company's internal e-mail system, which connected them to a local server, which is, in turn, connected to a worldwide server located in Singapore, which operates as a hub for all the company's local servers around the world. The employees all used as their e-mail address their name followed by the company's domain name, "*energizer.com*".

The following occurred when the employees transmitted or received e-mail. If they corresponded internally between

one another (or with a colleague in South Africa), the transmission would remain on and go no further than the local server. If they corresponded with a colleague internationally, the transmission would be transmitted from the local to the Singapore server, which would then post it to the applicable international server. Again, the transmission would remain on and go no further than the various internal servers if they corresponded with someone outside of the company (for example, a friend at another company in Johannesburg), the transmission would be routed from the local server to the server in Singapore, which would then post it out onto the worldwide Internet for transmission to the relevant domain name in South Africa. On every occasion that they received an incoming e-mail from outside of the company (again, for example, from a friend at another company in Johannesburg) sent to their Energizer domain name, the e-mail would be posted out onto the Internet, received, sorted and re-routed by the Singapore server to the local server, which would then allocate it to the relevant employee's local post box.

Although it did not have a specific e-mail policy, the following four documents served to establish (as the company ultimately argued) a rule against e-mail abuse. Firstly, an extract from its *Business Practices & Standards of Conduct* booklet dealing with environment policies, which outlawed (on pain of disciplinary action, "*which may include termination of employment*") behaviour creating an offensive working environment caused by "*disparaging or insensitive comments, actions, gestures, jokes or epithets, or the display of derogatory, obscene, demeaning or objectionable signs, posters, cartoons, photographs or drawings*" (the policy). The policy was displayed on the local notice board. Secondly, an e-mail from the company's head office in the USA sent to all South African users, which warned against cyberloafing and confirmed that the policy also applied to electronic communications. Thirdly, an e-mail from the company's MD (which he sent to all local users in response to having received a chain letter from one of the employees) reading: "*Please refrain from on-sending these ludicrous chain e-mails on company systems and company time!*" Fourthly, a provision in the employee's contracts of

⁶ The campaign included articles in the *Fair Lady*, the *Citizen* and the *Sunday Times*, participation by the employees' attorney in a *Radio 702* talk show, and even an appearance by two of the employees and their attorney on the *Toasty Show* on eTV.

employment, which placed a burden on them to apprise themselves of company policy.

Over a period of time, the company's communication costs (a large component of which comprises charges levied in respect of the Singapore server) rose significantly. This motivated the MD to call for the e-mail boxes of three of the employees (Bamford, Wollenschlaeger and Oosthuizen) from Singapore.

On receipt of the boxes (which contained many thousands of messages), the MD conducted a general overview thereof. He was concerned only with attachments and did not open and read personal e-mails, it not being his intention to acquire confidential information. The MD was immediately struck by the fact that the e-mail boxes of the three employees contained a vast collection of offensive material, and that the two other employees (Fume and Gibson) appeared to be involved in the communication ring as it was apparent that they were the source of some of the offensive material and that other of it had been sent to them by the three employees.

Within two days of this discovery, the MD had interviewed all employees at head office and at the company's regional offices in Cape Town and Durban. During the course of these interviews, two managers (one being a Mr Herbst) admitted that they had received (but not sent) offensive material from some of the employees. The balance of the staff complement assured the MD that they had not in any way abused the company's e-mail system.

Disciplinary charges (effectively of e-mail abuse) were then brought against the five employees and Herbst (no charges were brought against the other manager as he resigned).

The result of the ensuing disciplinary enquiries was that all concerned were found guilty and all of them, except for Herbst, dismissed. The following should be noted in this regard. Bamford, Fume, Gibson and Wollenschlaeger were found to have trafficked in offensive material, including some forms of pornography. Gibson was found in addition to have continued sending chain letters after the

MD's e-mail prohibiting same. Oosthuizen was only found guilty of continuing to send chain letters after the MD's e-mail prohibiting same, which was construed as a warning in her case as it had been pertinently directed at her as she had sent the offending chain letter to the MD that resulted in him prohibiting such conduct in the future. Herbst was found guilty only of having received (and not forwarded) offensive e-mail from the employees and was thus given a final warning instead of being dismissed.

- Preparation for arbitration

In preparation for the arbitration, the following transpired. The employees called for the discovery of the entire contents of their e-mail boxes together with copies of all the offending e-mails. They notified that they intended to raise an inconsistency challenge on the basis that six other employees (including Herbst and one Krugel) had sent and / or received offensive e-mail and had either escaped censure or (in the case of Herbst) only received a warning. On the basis of the foregoing, they also called for the discovery of the e-mail boxes of the six employees involved in the inconsistency challenge. They reserved the right to challenge the authenticity of the discovered material under the *Computer Evidence Act, 57 of 1983*, which provides that only "authenticated" computer-generated documents (which requires a detailed investigation into the accuracy of the data and reliability of the storage facility and printing mechanism) are admissible as evidence in civil proceedings.

This all caused the company some difficulty for, *inter alia*, the following reasons. Although in existence (they had been retained after they had been called for by the MD) the e-mail boxes of Bamford, Wollenschlaeger and Oosthuizen contained some 5000 messages, with there being no clear distinction between business and recreational e-mail, which, amongst other things, gave rise to legitimate concerns about the disclosure of confidential company information in the event of full discovery. The e-mail boxes of Fume and Gibson were automatically deleted (permanently) upon their dismissal, and could only be reconstructed with reference to the data contained in the

e-mail boxes of the other three employees (from which it could be determined if Fume and Gibson had sent / received offensive material to / from the other three employees). Given that they had also left the company, the e-mail boxes of two of the six employees involved in the inconsistency challenges also had to be reconstructed from those in existence. The e-mail boxes of some of the remaining four persons involved in the inconsistency challenges had been cleaned out in the intervening period in the ordinary course, but this nevertheless gave rise to suspicion on the part of the employees. In order to determine the authenticity of the material, each piece of material had to be carefully tracked.

In the circumstances, the company had no option other than to appoint an expert (in the form of Deloitte & Touche) to undertake a complete audit of the employees' e-mail and that of the persons involved in the inconsistency challenges. The experts set about making a division between business e-mail (which was put aside in the interests of confidentiality) and recreational e-mail (which they then classified into various categories for indexing purposes), determining the authenticity of the material and investigating the veracity of the employees' inconsistency challenges (which the employees gave precise details of during a pre-arbitration conference). Although this proved to be a hugely expensive and time-consuming exercise (some 160 hours of professional time was spent on the task), it ultimately served as the basis for the company's success as it effectively put paid to the employees' inconsistency challenges and those in relation to the authenticity and providence of the material in question.

By the time of the arbitration, the expert (who testified on behalf of the company) had compiled a full catalogue of all the relevant e-mail (the schedules alone ran to over 200 pages) and was able (with the use of a specially designed software program, and a digital projector) to call up and display any chosen item on a projection screen erected at the venue of the arbitration.

Having trawled through all the material, the company isolated approximately 80 items of offensive material that it intended

to rely upon, which material was classified into various categories (including pornography, sexually offensive, other offensive, trade mark violations, and chain letters). Expert opinion was obtained to establish the authenticity of each item, and both hard and soft copies of the material were discovered. The expert's catalogue and CD's containing the recreational e-mail of the employees and those involved in the inconsistency challenges were also discovered in advance, and the expert was retained to be of assistance to either of the parties when and if so required.

- The issues before the arbitrator

In relation to the substantive fairness of the employees' dismissal (the procedural challenges are not relevant for present purposes), the arbitrator was called upon to decide the following issues in relation to the three employees who proceeded with the case: whether or not there was a clear rule regulating the employees' conduct; if the rule existed, whether or not the rule was properly communicated to them; whether or not the employees contravened the rule; whether or not there was a clear sanction applicable to the contravention of the rule; if there was, whether or not the sanction was properly communicated to the employees; and whether or not the sanction of dismissal was applied appropriately and consistently.

In regard to the monitoring and interception of the employees' e-mail, the arbitrator was also tasked with having to determine: whether or not the company was entitled to monitor and intercept the employees' private e-mail; and if not, whether or not the evidence obtained was admissible.

- Summary of the arbitrator's findings on the merits

In his award, the arbitrator finds that Wollenschlaeger and Oosthuizen had involved themselves in a "*public smear campaign*" and lists a number of examples of false statements having been made to the press. Amongst others, he finds that the women never contended at arbitration that they were picked on because they were juniors and women, that Oosthuizen was not dismissed for sending bible verses and inspirational messages, and that the contention that certain of the

material was not pornographic “*flies in the face of any generally accepted definition of pornography*”.

In dealing with the material that formed the subject of the charges brought against the employees, the arbitrator describes a number of items of pornography, sexually offensive material, racially offensive material, trademark violations and chain letters. He finds that certain of the material is “*obviously contrary to what would circulate amongst self-respecting people*”, and that those of the jokes which have a racial connotation “*are typical of what one would strive to avoid in contemporary South African society*”. He goes on to describe the chain letters circulated by both Oosthuizen and Gibson as “*inane and vacuous*”, and finds their contention that they did not believe them to be chain letters untruthful.

The arbitrator rejected the claim by the women that there existed no clear rule prohibiting their conduct. He found that the company’s policy regulated the “*tone*” of the workplace, that “*it cannot lie in the mouth of well educated white-collar workers to say that they were unaware that it was impermissible for them to traffic in what was socially unacceptable material*”, and that even if there had not been a rule at all, “*it would follow from an application of common sense that images as grotesque as those described do not belong in the workplace and the applicants must have realised this fact*”.

Dealing with the applicants’ claim that they had not known that they could be dismissed for their misconduct, the arbitrator found that although dismissal was not prescribed in writing, the applicants’ misconduct damaged the business by “*clogging up the system and running up costs*”, there existed a foreseeable danger of the Energizer domain name being associated with offensive transmissions, there was a foreseeable and distinct likelihood of employees internally being offended by the material, and that “*any reasonable employee would not use company property for non-company business unless authorised to do so*”. The arbitrator concluded that the applicants ran the risk of dismissal upon commission of what was serious misconduct and that their denial of

an appreciation of this fact was not credible.

In regard to the applicants’ inconsistency challenges, the arbitrator found that “*the real issue in so-called ‘inconsistency’ is whether or not the employer has selectively picked who to discipline*” and that there was no evidence of this. Evidence had come to light to the effect that Herbst and Krugel may have been more involved than they had let on at the time of the MD’s investigation, but the company had undertaken to address the matter after the arbitration. Dealing with the applicants’ complaint that the company had not conducted a comprehensive investigation across the organisation and had focussed on the applicants alone, the arbitrator found that “*in the absence of demonstrating mala fides on the part of the management at the relevant time no material criticism can really be levelled at the employer for not having disciplined more people than it actually did*”.

Finally, the arbitrator turned to the question of sanction. He found that Oosthuizen and Gibson had openly defied a direct instruction to stop sending chain letters from their MD, which constituted an act of insubordination warranting dismissal. In regard to the involvement of Wollenschlaeger and Gibson in the trafficking of offensive material, this created the risk of the company being associated with these images, with the result that it could not be faulted for its loss of trust and confidence. The dismissal of all three of the remaining applicants was thus upheld.

- The invasion of privacy issue

The employees sought to exclude all the e-mail evidence on the basis that the obtaining thereof involved an unlawful invasion of their privacy.

They relied on section 2(1) of the *Interception and Monitoring Act, 127 of 1992* (the IMP Act), the relevant part of which reads:

“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.*⁷

They also cited section 14 of the Constitution, which includes the provision that:

“Everyone has the right to privacy, which includes the right not to have - ...

- (d) *the privacy of their communication infringed.”*

The mischief that the IMP Act addresses is illicit eavesdropping, with the aim being to obtain confidential information. As was argued before the arbitrator, such mischief did not arise in *Energizer*.

The MD testified that he had investigated certain e-mail boxes after continuing problems with rising expenses including, in particular, the charges levied in respect of the Singapore server. It was not at any time his intention to acquire confidential

⁷ A new draft *Interception and Monitoring Bill* has been published recently (<http://www.polity.org.za/govdocs/bills/2001/draftintercept.html>). While section 2(1) remains unaltered, subsections (2) and (3) represent innovations. Subsection (2) reads: “Any person may monitor any communication by means of a monitoring device where – (a) such person is a party to that communication; or (b) one of the parties to the communication has consented to such monitoring.” Subsection (3) goes on to provide: “Any person who is a party to a communication may, in the course of the carrying on of any business and without the knowledge or permission of the other party to that communication – (a) intercept the communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications system; or (b) monitor the communication by means of a monitoring device, for the purpose of monitoring or keeping a record of – (i) any communication by means of which transactions are entered into in the course of that business; or (ii) any other communications relating to that business or taking place in the course of it being carried on.”

information about any of the employees. He did not open and read personal e-mails, his concern being with those that had attachments. In short, the e-mail examination did not in any meaningful way amount to illicit eavesdropping.

Moreover, the material that became revealed in the course of the examination was not of the nature to which the law would accord the attribute of confidentiality as it was effectively in the public domain. The material was not such that the employees could have harboured a legitimate expectation of privacy.⁸

It was also relevant⁹ that the employees knew that there was no cocoon around their traffic in non-business e-mails. Wollenschlaeger testified that she had gathered from the e-mail from the company’s head office in the USA that the company would scan employees’ computers if a need to do so arose, and that she chose nevertheless to send out the offensive material that led to her dismissal. In such circumstances, she could not lay claim to the confidentiality of the information.¹⁰

It was also argued before the arbitrator that recourse to the Constitution did not strengthen the position of the employees, and that, in any event, the arbitrator retained a discretion to admit evidence, even where the obtaining of it carries some taint.¹¹

The arbitrator dealt with the issue crisply in his award. He records that the company did not enquire into personal communications and that the offensive material had been generated by anonymous third parties and distributed for consumption on the Internet. He goes on to conclude:

⁸ Cf *Lenco Holdings Ltd & others v Eckstein & others* 1996 (2) SA 693 (N) at 700; *Protea Technology Ltd & another v Wainer & others* 1997 (9) BCLR 1225 (W) at 1239H; and *S v Kidson* 1999 (1) SACR 338 (W) at 348. By way of contrast, see *Geerdts v Multichoice Africa (Pty) Ltd* [1998] 9 BLLR 895 (LAC), which involved a clear-cut case of illicit electronic surveillance.

⁹ In the context of the analysis by Heher J in *Protea Technology* (fn. 8 above).

¹⁰ It warrants mention that Bamford mentioned on the *Toasty Show* that she had no difficulty with the company having monitored her e-mail because she had done nothing wrong.

¹¹ *Protea Technology* (fn. 8 above) at 1237E-1244C.

*“In no sense whatsoever has the personal dignity or personal affairs of any of the applicants in the least been disturbed. Furthermore, all the information which was the subject matter of the proceedings was derived from storage facilities in the company’s own e-mail system. It can hardly be said, even in respect of genuinely ‘personal’ communications, that individuals are entitled to deposit intimate material in their employer’s storage facility and require their employer not to examine it in order to determine whether there is any point to having it kept”.*¹²

LESSONS TO BE LEARNT

Although it was successful, the task of defending the company was made significantly more difficult through the absence of a comprehensive and self-standing electronic communications policy. The primary lesson to be learnt from *Energizer* is that such a policy is absolutely imperative, with the benefits being that: firstly, it serves to overcome challenges to the existence of a rule prohibiting e-mail abuse, knowledge of that rule, the appropriate penalty for a breach of the rule, and knowledge of that penalty; secondly, it serves to assist in avoiding inconsistency challenges by setting a standard against which the conduct of employees is measured and by being a tool to persuade employees against committing such misconduct; and thirdly, and importantly, a policy that deals properly with the right of the employer to monitor employee e-mail will go a long way to negating challenges to the admissibility of evidence on this front.

The next major lesson is that the policy must be workable. *Energizer* is illustrative of the fact that it is unsustainable to absolutely prohibit employees from using the Internet / e-mail for private purposes. It is surely more efficient for employees to use e-mail (instead of making a telephone call, sending a fax, or taking a short trip out of the office) to conduct that range of personal affairs ordinarily allowed by employers during working hours. To

prohibit them from doing so may not only prove to be counter-productive, but it may also prove to be unenforceable simply because such a prohibition will probably be regularly flouted by many employees and thus lead to inconsistency challenges in the event of a dismissal based upon a breach of the prohibition. As far as we are concerned, a reasonable degree of private use must be allowed. *Energizer* also demonstrates that to be workable, an e-mail policy must place restrictions on both the forwarding and receipt of offensive e-mail – those who receive it cannot be treated as innocent involuntary participants in the transaction. Although they were unsuccessful, the employees in *Energizer* alleged that, like them, their managers could not have known about the existence of a rule prohibiting the forwarding of offensive e-mail and could not have considered it to be a dismissible offence because the employees sent offensive material to their managers and they did nothing about it. To avoid this type of situation arising, an obligation must be placed on those who receive offensive e-mail to report the matter or otherwise attend thereto.

The third major lesson is that irrespective of the content of an electronic communications policy, in order for employees to adhere thereto, they need to understand the rationale behind and be constantly reminded of the policy. The employees in *Energizer* contended that they did not think that they could be dismissed because they did not know of the serious implications of their conduct. While they were unsuccessful in this regard, it would be prudent to get employees to buy into an electronic communications policy through a process of educating them about the potential evils of e-mail. The major problem with getting employees to adhere to an electronic communications policy consistently is that they perceive (often inadvertently) that they effectively own the computer on their desk and can thus use it as they please. To overcome this, employers would be well advised to constantly reaffirm the policy with employees. Some innovative measures have been resorted to, including the printing of the policy on mouse pads and the programming of computers in such a way that employees can only gain access thereto after having confirmed their commitment to the policy on screen.

¹² See further regarding the issue of privacy, Carl Mischke “*The Monitoring and interception of electronic communications: Obtaining and using e-mail and other electronic evidence*”, *Contemporary Labour Law* vol. 10, no. 10, May 2001.

The final major lesson relates to the security of information and its storage in the context of having to defend a dismissal for e-mail abuse at arbitration before the CCMA. It can be expected that an employee charged with e-mail abuse will often place the authenticity of the e-mail and the company's records in relation thereto in question, which was the stance initially taken up by the employees in *Energizer*. Such challenges may include that the employee was not the source of the offending e-mail, that he did not forward or receive it, that it was planted in his e-mail box by the systems administrator or by someone having access to his password, etc.

So as to avoid the expense that Energizer was put to in this regard, it is important that employers have consideration to these sorts of issues and put the necessary safeguards in place in advance of such a challenge. It must be understood that the introduction of an e-mail transaction report does not in itself establish that the employee was guilty of effecting the transaction recorded therein. *Energizer* would have been a much easier case if the company had been in a position in preparing for the arbitration to restore the e-mail of the five dismissed employees and of the six employees involved in the inconsistency challenges as at the date of the employees' dismissal. If this had been possible, it would have saved the company from having to reconstruct a number of e-mail boxes and would have avoided the suspicion that arose as a consequence of the fact that the e-mail of various employees involved in the

inconsistency challenges had been cleaned out (albeit in the ordinary course) during the intervening period. While there are compelling considerations in favour of an employee's e-mail record being deleted immediately upon him leaving a company's employ and in favour of employees being allowed to manage their e-mail through the deletion thereof, it may be prudent to have consideration to keeping a back up of deleted e-mail for the reasons mentioned.

Goldman Judin Maisels Inc represented Energizer in the arbitration dealt with herein.

We can be contacted on: (011) 447-8177 (tel); (011) 447-8122 (fax); or law@elawnet.co.za. Visit our website: www.elawnet.co.za.