MONITORING EMPLOYEE USE OF E-MAIL AND THE INTERNET

Elizabeth J. Forster
Blaney McMurtry LLP
416.593.3919
eforster@blaney.com

MONITORING EMPLOYEE USE OF E-MAIL AND THE INTERNET

1. INTRODUCTION

Personal computers have become a fundamental tool in most workplaces.

A recent article in ***ca magazine***[1] cited a study by International Data Corporation which showed that in 1996 in the United States, 47% of all US businesses and 60% of companies with over 500 employees had e-mail in the workplace. Yet only 18% of these companies had written policies to deal with employee use of e-mail. Businesses using the Internet has grown rapidly since that time. By May 1999, surveys showed that 60% of all Canadian employers provided Internet access to their employees [2]. Nevertheless, the proportion of these employers with written Internet policies remains very low.

The use of the computer and, in particular, the use of the e-mail and Internet systems, creates many legal issues for employers and employees. Unfortunately, there is no legislation and few court cases dealing with these issues to provide guidance to employees on this subject.

This paper will summarize some of the employment issues that arise because of employee use of e-mail and the Internet in the workplace and suggest appropriate mechanisms for dealing with these issues.

2. ISSUES RAISED BY E-COMMERCE

(a) Privacy

This particular area has received more attention in the United States and in some provinces outside of Ontario which have enacted privacy legislation.

There is no privacy legislation in Ontario. However, in recent years the Ontario courts have recognized a common law right to privacy. In ***Roth et al v. Roth et al*** (1991), 9 C.C.L.T. (2d) 141, Mandel J. adopted a decision of the Supreme Court of Canada in defining the right to privacy as "the right to be secure against encroachment upon citizens' reasonable expectation of privacy in a free and democratic society.[3] However, Mandel J. also held that not all invasions of privacy give rise to a legal remedy. Rather, a remedy was only available if "the invasion is substantial and of a kind that a reasonable person of normal sensitivity would regard as offensive and intolerable."[4]

The right to privacy has also been recognized in the labour context for some time. Most arbitrators have held that employers have no right to violate an employee's right to personal privacy by searching an employee unless the employer has established adequate cause for the search.

A summary of the position taken by most arbitrators is found in ***Re Loomis Armoured Car Service Ltd.*** (1997), 70 LAC (4th) 400 where the arbitrator, in dealing with the refusal of an employee to submit to a polygraph test held at page 409:

> I begin my analysis with first principles. As Arbitrator Michel Picher pointed out in ***Re Monarch Fine Foods Co.***

> ***and Milk and Bread Drivers, Dairy Employees, Caterers and Allied Employees, Loc. 647*** (1978), 20 LAC (2d) 419, when a person becomes an employee she or he does not give up the right to integrity of the person. That case concerned a medical examination but the remarks are equally useful here.
>
> It is well established that persons do not by virtue of their status as employees lose their right to privacy and integrity of the person. An employer could not at common law assert any inherent right to search an employee or subject an employee to a physical examination without consent: ***Latter v. Braddell et al.*** (1881), 50 L.J.Q.B. 448 (C.A.). Thus there is nothing that can be described as an inherent management right to subject an employee to what would otherwise be a trespass or an assault upon the person**…**

Even in cases of suspected employee theft, arbitrators have limited an employer's right to search:[5]

> There is no dispute that the law on personal privacy in the work place establishes that an employer does not have an absolute right to search an employee or the employee's personal belongings. There is no contractual provision relevant here which might override that principle. Unless an employer has reasonable ground to believe that the employee is in possession of company property without authorization, it cannot conduct a search of an employee or his or her personal belongings; where an employer does have reasonable ground for thinking that the employee has committed theft, it should obtain police assistance if the employee refuses a search rather than search the employee**...**

To date there is no case law in Canada dealing with the privacy of employee e-mail communication. In the United States, most courts have taken the view that as the computer system was the property of the employer, the employer had a right to search the system at any time and as such, employees had no reasonable expectation that their e-mail communications would be private.

For example, in ***Smyth v. The Pillsbury Co***. (1996), 914 F. Supp. 976, an employee used a company e-mail system to refer to the sales management of his employer and threatened to "kill the backstabbing bastards". He was terminated. Under U.S. law, he was an "at-will employee" and therefore, not entitled to notice of his termination in any event. He therefore sued his employer for wrongful discharge alleging an invasion of his privacy. The court dismissed his action and found that there was no reasonable expectation of privacy in the e-mail communications over a company-wide e-mail system. The court said:

> …we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management.
>
> …even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy.

In ***McLaren v. Microsoft Corporation*** (1999) WL 339015 (Tex. App), an employee was terminated by Microsoft Corporation for using the e-mail system for sexual harassment. The employee sued Microsoft for invasion of his privacy by reviewing his e-mail. The Court dismissed the lawsuit holding that "e-mail messages contained on the Company computer were not McLaren's personal property, but were merely an inherent part of the office environment".[6]

It is likely that the employer has a right to search an employee's e-mail as part of its right to control the workplace. Further, the employer can in most circumstances assert the fact that it owns the computer system. However, until we have guidance from legislation or from the Ontario courts, employers are cautioned to advise employees in writing that their e-mail communications may be reviewed by the employer at any time.[7]

(b) **Employer Liability**

The technology now exists to search e-mails even once they have been deleted. This technology has become a powerful tool in litigation. In a recent article entitled ***"Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age"***,[8] the authors cite some interesting examples of situations where employers have been exposed to liability as a result of a legal requirement that they produce all e-mail messages in their system.

In one case, a woman sued her former employer for termination as a result of age discrimination. The employer denied the allegation, but was ultimately forced to settle the case for $250,000.00 when an e-mail message from the Company's President to the head of personnel was disclosed in the course of a lawsuit . The e-mail instructed the head of personnel to "get rid of the tight assed bitch".

In ***Re Air Disaster at Lockerbie, Scotland***, 37 F. 3d 804, a jury verdict against Panamerican World Airways for damages as a result of the airplane crash over Lockerbie, Scotland was upheld by the court. In order to be successful, the plaintiff had to prove wilful misconduct on the part of Panamerican World Airways. The Plaintiff succeeded

because it was able to obtain copies of e-mail messages from company management to all security personnel advising them that they did not have to follow the regulations requiring the use of x-ray and personal searches of baggage.

In short, employees and employers must exercise great caution with respect to this type of information communicated by e-mail any should consider limiting the type of information that can be sent by E-mail.

(c) **Human Rights**

The ***Ontario Human Rights Code*** prohibits both discrimination and harassment in the workplace because of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, age, record of offences, marital status, family status and handicap.

There is an enormous proliferation of pornographic, sexually explicit and racist material distributed over the Internet system. When this material is distributed or displayed in the workplace, it may constitute harassment contrary to the ***Ontario Human Rights Code***.

For example, in ***DiVito v. Macdonald Dettwiler & Associates***, [1996] B.C.J., No. 1436 an employee used the company's e-mail system to circulate a derogatory sexual description of another employee. The employee was dismissed and the dismissal was upheld by the court because the employee lied about this involvement: The trial judge held:

> …I am not persuaded that the conduct of the plaintiffs, so far as their involvement in the distribution of the e-mail message is concerned, is alone sufficient grounds for their summary dismissal. I am of the view that, standing alone, that conduct warranted a severe repremand, but nothing more.
>
> However, such conduct, when combined with the plaintiff's subsequent dishonesty during the investigation, does in my opinion, clearly amount to just cause for dismissal.

In ***Re Prasad A. Bhame*** [9]a Board of Referees appointed under the ***Employment Insurance Act*** confirmed that an employee had been terminated for misconduct and therefore ineligible for benefits for distributing obscene "notes" on the company's e-mail system.

In Dorrian and Canadian Airlines International Ltd.[10] an adjudicator appointed under the ***Canadian Labour Code*** dealt with a claim of unjust dismissal brought by a person who was dismissed for cause for among other things, workplace harassment and possession of inappropriate materials on company premises. The adjudicator upheld the dismissal and stated:

> … it is my view that the act of downloading and storing pornographic material on a company computer, the act of keeping pornographic material in the office, and the act of using company stationary to correspond with an adult magazine constituted the "unauthorized use of company property"…

It is important that workplace harassment and sexual harassment policies also be updated to prohibit dissemination of discriminatory and sexually explicit material over the e-mail system so as to avoid any suggestion that the employer permitted a "poisoned work environment".

(d) **Defamation**

Employers should also be concerned about potential liability for defamatory statements sent out on their e-mail system.

Defamation occurs when a person communicates material to another which is untrue and likely to disparage another person [11].

Not only can defamatory comments be spread about existing employees on the E-mail system, but disgruntled employees may make such comments public through the Internet system. There legal remedies available in the case of the latter concern are unsatisfactory at present. However, careful monitoring of the E-mail system can at least minimize the use of offensive inter-office communication.

(e) **Disclosure of Confidential Information and Trade Secrets**

Great concern has been expressed about the disclosure of confidential information or trade secrets over the Internet system. Disgruntled employees can disseminate all kinds of sensitive information over the Internet. In addition, sensitive e-mails can potentially be intercepted by third parties. Employers may wish to either prohibit this type of information from being sent on the Internet, or alternatively, monitor E-mail messages closely.

Employers should also caution employees not to download material subject to copyright which could expose the company to a claim of breach of copyright.

(f) **Failure to attend to Business**

Recent studies have shown that 24% of the time spent by employees on-line was not work related. For example, in the United States, businesses lost $450,000,000.00 in work productivity when the Starr Report on President Clinton was released.

Lack of productivity is very expensive. However, it is often difficult to monitor what employees are doing at their computer as it appears that they are hard at work even though they may be engaged in other activities.

A recent article in the ***Report on Business Magazine*** [12] cites a report by Surf Watch in California which concluded that 1/3 of all time spent by employees surfing the Internet is personal, 50% of employees shop on-line while at work and 90% of employees surf "recreational" sites while at work.

Once again a carefully drafted policy will at least serve to make it clear to employees that personal use is either not permitted or must be limited.

3. **POLICY**

Many of the legal issues involving employee e-mail use and the uncertainties surrounding these issues can be resolved by use of a carefully drafted e-mail policy.

The policy should clearly set out the employer's expectations with respect to e-mail and Internet use in clear concise language. A copy of the policy should be given to all employees and employees should be asked to acknowledge in writing that they have read and understood the policy as a condition of use of the company's e-mail and Internet

system. We also recommend that this process take place on an annual basis so that employees are regularly reminded of their employer's expectations.

At a minimum, all policies should address the following points:

(a) The computer system is the property of the employer and the employer retains ownership of all files, documents and communications received, created or stored by employees in the system;

(b) The computer system is to be used for the purposes of the employer's business only;

(c) The e-mail system must not be used to transmit, view or store obscene, defamatory, discriminatory, pornographic, threatening, sexually explicit, harassing or any other offensive material;

(d) The e-mail system must not be used to duplicate or transmit material over which a copyright may be claimed without the consent of the owner of the copyright;

(e) No confidential information nor trade secrets belonging to the employer should be transmitted over the Internet;

(f) The employer may monitor any e-mail communication and internet usage at any time;

(g) A warning that a mere deletion of a message or file may not fully eliminate the message from the system;

(h) A statement that a violation of the policy will lead to discipline up to and including discharge; and

(i) An acknowledgement that the employee has read and understood the policy.

4. SUMMARY

Enforcement of appropriate employee conduct regarding the use of e-mail and the Internet follows the same basic employment principles that are applied in all other situations where it is necessary to regulate employee conduct. In short, employers should have clear policies setting out what is expected of employees. Employers should ensure that employees have read the policy, understand the policy and are constantly reminded of the policy to reinforce the importance of them.

ENDNOTES

1. Rosie Lombardi, "Corporate Confidential". *ca magazine* June/July 1998.

2. Lia Chiarotto, "Reducing the Risk of Employer Liability for Internet and E-mail Misuse by Employees" *Employment and Labour Law Reporter*, May 1999 Volume 9, No.2.

3. *Canada (Director of Investigation and Research Combines Investigation Branch) v. Southam Inc*., [1984] 2 SCR 145 at page 159.

4. Fleming, *The Law of Torts*, 7th ed. (Sydney: Law Book, 1987), at p. 575.

5. *Re Brampton Hydro* (1991), 23 LAC (4th) 126 at page 128;

6. Anne Lehman, "E-mail in the Workplace: Question of Privacy, Property or Principal?". *The Catholic University of America Com Law Conspectus* 5 Common Law Conspectus 99.

7. Holly L. Rasky,. "Can an Employer Search the Contents of its Employees' E-mail?", 20 Advocats Quarterly, 221.

8. Mark Dichtes, M.S. Borkhardt, "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age".

9. CUB 42012A, March 17, 1997.

10. [1997] C.L.A.D. No. 607.

11. *Clark & Lindsell on Torts* (London: Sweet & Maxwell, 1995) at page 1009.

12. Clive Thompson, "*Bang on that Drum All Day*". Report on Business Magazine March 2000.