

FRANCHISING AND THE USE OF CYBERSPACE IN THE WORKPLACE

Christopher Deehy
christopher.deehy@lapointerosenstein.com
Lapointe Rosenstein
Montreal, Quebec

with the collaboration of:
Anne-Marie Gauthier, Lapointe Rosenstein
and
Jonathan Wilson, King & Spalding

Cyberspace¹ is rapidly becoming an integral part of any contemporary business. Though the advantages of its use are numerous, it also poses certain risks. From a human resources perspective, the use of cyberspace technology creates new situations where problems may arise that must be addressed by franchisors in their capacity as employers. Consequently, the authors recommend that franchisors consider these issues now, and adopt and formulate a policy before problems arise. Adopting a cyberspace policy allows employers to take the initiative by both avoiding potential liabilities and by educating employees on the efficient use of cyberspace technologies. A cyberspace policy should inform employees of the risks of copyright violations, trade secret protection and the inadvertent loss of company intellectual property assets. It should also guide employees on the appropriate use of E-Mail and similar technologies in combination with an appropriate sexual harassment education program.

For franchisors, cyberspace technology can be a vehicle by which information regarding operating methods, updates to the operations manual and accounting systems can be rapidly disseminated to franchisees. However, the fact that cyberspace is such an effective means of disseminating information brings new concerns to franchisors, primarily regarding security and the protection of proprietary information. Consequently, when franchisors consider formulating a policy regarding the use of cyberspace in the workplace, they must bear in mind that such a policy cannot be effectively implemented without franchisee participation. Thus it would be advisable for franchisors to also include a cyberspace policy in their operations manuals.

This article addresses the developing law of cyberspace in the workplace in both Quebec, Canada, and the U.S. In the first portion of the article key issues of concern to employers are outlined, while in the second portion a checklist for a comprehensive workplace cyberspace policy is created.

1. THE LEGISLATIVE FRAMEWORK

1.1 In the Province of Quebec, Canada

Private contractual relations in Quebec are governed by the *Civil Code of Quebec* (the "*Civil Code*"), which draws its sources from French Civil law. Employment contracts are governed by Chapter 7 of the *Civil Code* and the other general rules applicable to contracts provided therein. Those provisions are supplemented by statutes that also create obligations for employers. For companies whose activities in Quebec fall under provincial labour jurisdiction (i.e. the vast majority of employers), the principal sources of statutory obligations are the *Charter of human rights and*

*freedoms*² (the "Quebec Charter"), the *Act respecting occupational health and safety*³ and the *Act respecting the protection of personal information in the private sector*⁴.

1.1.1 Health and Safety

Section 51 of the *Act respecting occupational health and safety*⁵ states that the employer must take the necessary measures to protect the health and ensure the safety and physical integrity of the employee. Article 2087 of the *Civil Code* requires an employer to take measures to ensure the protection of the health and safety of the employee and reads as follows:

"The employer is bound not only to allow the performance of the work agreed upon and to pay the remuneration fixed, but also to take any measures consistent with the nature of the work to protect the health, safety and dignity of the employee."

Section 46 of the *Quebec Charter* states that every employee has a right to fair and reasonable working conditions:

"Every person who works has a right, in accordance with the law, to fair and reasonable conditions of employment which have proper regard for his health, safety and physical well-being."

These three legal sources create an obligation for employers to ensure that their employees are working in an environment that is secure and where they will be free from harassment.

1.1.2 Vicarious Liability

Article 1463 of the *Civil Code* states that an employer is liable to repair for injury caused by the fault of its employees in the performance of their duties. This article has the effect of establishing a regime of vicarious liability for employers. If the employee commits a fault in the performance of his duties, then the employer is automatically liable for any damages that are a consequence of same.

1.1.3 Privacy

An individual's right to privacy is protected by Section 5 of the *Quebec Charter*. It should be noted that the *Quebec Charter* guarantees rights and freedoms to individuals in their dealings with the state and in private contractual matters as well; such as employment contracts between private parties. It is a statute that is invested with quasi-constitutional status, which means that when interpreted by the Courts, it takes precedence over other legislative or contractual provisions that are contrary to it. The fact that the right to privacy is contained in the *Quebec Charter* means that it is considered to be wellnigh constitutionally guaranteed. Furthermore, Article 35 of the *Civil Code*, adopted in 1994⁶, reinforces the right to privacy by stating that every person has the right to the protection of his reputation and privacy and that no one may invade the privacy of a person without that person's consent. The act of invading a person's privacy constitutes a civil fault that renders the author of the violation (or his employer depending on the circumstances) liable for damages. Article 36 of the *Civil Code*⁷ stipulates that the act of intentionally intercepting or using an individual's private communications may be considered as an invasion of an individual's privacy. Thus, the reading of E-Mail by an employer may, *a priori*, be considered as constituting a violation of the employee's privacy.

Finally, the *Act respecting the protection of personal information in the private sector* (the "Act") adopted in conjunction with the *Civil Code* to ensure the protection of the right to privacy, also creates obligations for the employer with respect to the protection of personal information regarding its employees and former employees. It prohibits an employer from releasing personal information regarding an employee to third parties without the employee's prior consent and creates obligations for employers with regards to the storage and disposal of personal information that is no longer useful. Any violation of the employer's obligations under the *Act* can render him liable, vicariously or directly, for damages caused by such violation.

1.1.4 Canadian Case Law

Canadian employment case law that has expressly addressed cyberspace issues is scarce. Most of it has been rendered either by administrative tribunals such as labour arbitrators, generally under collective agreement grievance arbitration, or by the trial courts adjudicating unjust dismissal cases. The appellate level courts have not really dealt with the substantive issues as of yet. However, the cases can serve as an illustration of the problems that unregulated use of cyberspace can create for employers.

In the matter of *Di Vito vs. MacDonald Dettwiler and Associates Limited*⁸, two employees were dismissed following the discovery by their employer of their involvement in distributing offensive material about a co-worker via E-Mail. The E-Mail made reference to a specific female employee who suffered from a serious weight problem. It had been sent by one of the dismissed employees to the other and stored for more than a year. That employee then forwarded it to several other employees and posted it on a company bulletin board, turning the matter into one of public harassment. When confronted with their actions, the employees denied any wrongdoing.

The Court held that the fact that the E-Mail had been stored for a lengthy period of time and then revived was an aggravating factor as it demonstrated that the decision to send the E-Mail was not the result of a momentary lack of judgment. The Judge ruled that the employees' conduct in distributing the E-Mail was not in itself sufficient grounds for a summary dismissal but that when combined with the fact that the employees had refused to disclose their wrongdoing when confronted with it, warranted the termination of their employment.

In the case of *Canadian Pacific Limited and Transportation Communications Union*⁹, an employee was disciplined for having made improper use of the employer's E-Mail by sending messages containing derogatory comments about a co-worker, and for having accessed the employer's E-Mail system without authorization. The Union argued that the employer had failed to establish that it had properly communicated a clear policy of rules regarding what it considered to be improper or personal use of its E-Mail system. The employer did produce evidence to the effect that it had sent a notice via E-Mail to all E-Mail users advising them that frivolous or excessive personal use of the E-Mail was prohibited, but the arbitrator held that the employer had failed to meet its burden of proof by establishing categorically that the grievor had in fact received the communication (the employer was unable to bring evidence establishing that the employees had acknowledged receipt of the communication). The labour arbitrator also held that the employer's policy was unclear in the sense that it suggested that some personal use of the E-Mail system was permissible.

In a similar case, *Frezza and C.P. Rail*¹⁰, an employee was dismissed after it was discovered that he had made unauthorized use of the employer's computer system by illegally accessing his superior's E-Mail. A message informing users that unauthorized use of the system was subject to legal action including criminal prosecution under the *Criminal Code* appeared on

computer screens whenever users logged in, and the employee had already been formally warned once of the potential consequences of unauthorized use.

The arbitrator held that the message that appeared on the screen established that the employee knew that unauthorized use was prohibited. In the arbitrator's opinion, this breach coupled with the fact that the employee had already been formally warned once of the potential consequences of unauthorized use, warranted a dismissal.

Finally, in the matter of *Dufresne and Pratt and Whitney Canada Inc.*¹¹, an employee was dismissed after a charge of sexual harassment had been filed against him by another employee. The Labour Commissioner¹² concluded that no harassment had occurred and consequently reinstated the employee in his employment. The case is of interest because in its attempt to demonstrate that it had cause to dismiss the employee, the employer filed the results of an E-Mail audit that it had conducted of the employee's E-Mail bank records while investigating a prior complaint that had been filed against him. The complainant, a woman, had alleged that the male employee had repeatedly sent her E-Mail messages inviting her to go out with him but the audit revealed that the male employee had been sending messages of a sexual nature to two other employees within the organization (who had not filed complaints). The judgment makes no mention of whether or not the employer had a policy regarding E-Mail audits; however, the Labour Commissioner allowed the results of the audit to be filed into the Court record as evidence.¹³

1.2 In the United States

The developing body of law in the U.S. governing cyberspace in the workplace is growing on both the state and federal levels. In contrast to the Canadian system, applicable U.S. law can be found in both federal and state statutes and in the common law. As a consequence employers must regulate their workplace strategies, conservatively, mindful of the potential for inconsistent treatment by courts across state lines and between the state and federal systems.

U.S. employers should view the risk of employees' use of cyberspace from two perspectives: (1) the potential creation of liability for employers, and (2) the potential loss of or damage to employer assets. Somewhat in contrast to the situation under Canadian law, these issues have been explored in great length in the U.S. and there are numerous scholarly articles providing helpful analysis and resources.¹⁴

1.2.1 Liability

Employee use of cyberspace can create liability for employers in several ways. Intellectual property infringement is one of the easiest liabilities to identify. The easy availability of software and copyrightable text and images make possible the downloading and distributing of these materials from Internet sites. Downloading, and even printing material from an Internet site, may violate the copyright of the site's owners.¹⁵ If an employee downloads and distributes materials from an Internet site within the scope of the employee's duties to the employer, the employer may be liable for claims of infringement arising from that act.¹⁶ This can be especially dangerous in the era of private company-wide «Intranets» that post information for transmission to and copying by hundreds or thousands of company employees. Each copy made from a bulletin board service, like an Intranet, is a separate copy and a separate act of infringement for which the sponsor of the bulletin board may be liable¹⁷.

Cases have also arisen where employees' use of E-Mail has been used by other employees to support employment discrimination claims.¹⁸ Some studies have claimed that as many as twenty percent of E-Mail users have received sexually harassing E-Mail.¹⁹

Employers can also be found liable under the *Electronic Communications Privacy Act* and under various privacy tort theories if they monitor the E-Mail usage of their employees under certain circumstances.²⁰ Generally, the ECPA prohibits the employer monitoring of employee telephone calls except where the employee has consented to the monitoring²¹ or where the call being monitored is being made on a business telephone in the ordinary course of business.²² The ECPA also covers employer monitoring of E-Mail.²³ Unlike the treatment of telephone conversations, however, the ECPA gives employers a broader right to review employee E-Mail transmissions.²⁴

Some states have also enacted employee privacy-type statutes that are more restrictive than the ECPA.²⁵ Employers should review the applicable state statutes in those jurisdictions where they have significant operations if they plan to monitor employee use of cyberspace.

In addition to statutory authorities, however, some courts have addressed claims by aggrieved employees against employers under various privacy tort theories. The court in *Flanagan v. Epson America Inc.*, for example, rejected plaintiffs' claims that Epson's monitoring of employee E-Mail violated a common law "expectation of workplace privacy."²⁶ Likewise a federal district court in Pennsylvania rejected invasion of privacy claims made by an employee who was terminated by his employer for making unprofessional and inappropriate comments about other employees on a company E-Mail system, even where the company had assured employees that their E-Mails would be private.²⁷ Despite these victories for employers, however, employers should sensitize managers to the litigation risks posed by the inappropriate use of E-Mail.²⁸

1.2.2 Assets

Employers can find that valuable corporate assets are lost or damaged through the improper use of cyberspace by their employees.

The easiest example to identify is the loss of confidential information and trade secrets. Under the *Uniform Trade Secrets Act*, adopted in most states, a trade secret is:

"Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

A trade secret ceases to be entitled to legally enforceable protection when it is disclosed to a third party who has no duty to keep it secret.²⁹ Several courts have held that trade secret status is lost when a trade secret is exposed to the public on the Internet.³⁰ Establishing an electronic communications policy will not only warn employees of the dangers to the company of the inappropriate use of cyberspace but will also itself constitute evidence of the company's

exercise of "efforts that are reasonable under the circumstances to maintain [the] secrecy" of the company's trade secrets.³¹

Another example involves the inadvertent waiver of the attorney/client privilege. Generally, the attorney/client privilege cannot be asserted by a client if a third party (or "eavesdropper") has intercepted the communication. Some courts have reasoned that the privilege should not be lost if the attorney and the client reasonably expected their communication would be private, even though the eavesdropper succeeded in intercepting the communication. It is not clear, and there is no definitive case law deciding, whether attorneys and clients have a reasonable expectation of privacy in connection with communications that take place over public Internet circuits.³²

Similarly, the attorney/client privilege can be lost if otherwise privileged attorney/client communications become mixed with non-privileged business communications. For example, advice from an attorney to a working group of business persons by E-Mail might be forwarded to other business persons electronically, with business persons adding comments or additional information with each subsequent transmission. While the initial communication may have been privileged, the final version of the text, which contains non-lawyer to non-lawyer communications, may be found not to have retained its privileged status.

A related concern is the coordination of employer document retention programs with E-Mail retention by employees. Corporate document retention programs provide for the saving of different types of documents for different periods of time and the destruction of documents once the prescribed retention period has passed. Employees who save E-Mail messages for periods of time that are different from those prescribed by the document retention policy may subject the employer to significant expense if the employer is required, in a litigation context, to search for E-Mail messages falling within the scope of a discovery request.³³

2. CORPORATE POLICY CONCERNING THE USE OF CYBERSPACE

An effective company cyberspace policy should both educate employees regarding proper and improper use of company facilities, as well as create the legal justification for employee discipline and loss avoidance strategies. While there is no perfect cyberspace policy - indeed, the advisability of a particular policy will depend on the nature of the company's business and even the type of work done by particular classes of employees - nearly every effective policy should address the following issues:

2.1 Purpose and Scope

2.1.1 The policy should identify and articulate its rationale for existence and set forth the business justification for itself.

2.1.2 The scope of the policy should be clear. Will the policy apply only to employee use of company facilities? Will the policy apply equally to all levels of employees?

2.1.3 The policy should identify and describe the potential for discipline. Will all violations of the policy result in a reprimand? Is it possible for a violation of the policy to result in dismissal?

2.1.4 Will employees be required to consent to electronic monitoring as a condition of employment? If so, how will such consent be documented?

2.2 Use of Company Facilities

- 2.2.1 How, if at all, may company computer facilities be used for non-business purposes?
- 2.2.2 What categories of employees will have E-Mail? Internet access?
- 2.2.3 Will the company monitor employee E-Mail? If so, will monitoring be on a random basis or only in response to a specific suspicion of wrongdoing by an employee?
- 2.2.4 May employees install non-company software on company computers?
- 2.2.5 What person or group will enforce the policy? The Human Resources Department? The Information Systems Department?

2.3 Acquisition of Software and Intellectual Property Assets

- 2.3.1 Will employees be permitted to download software or other materials from Internet web sites? What restrictions, if any, will the company impose on such activities?
- 2.3.2 How, if at all, may employees use software obtained through the Internet (also known as "shareware" or "freeware") for company projects?
- 2.3.3 What limits, if any, will the company impose on Internet sites that may be visited by employees on company computers?
- 2.3.4 How will the company educate its employees regarding these rules? How will it enforce them?

2.4 Distribution of Company Information

- 2.4.1 If the company will have a web page, what persons will review and approve content to be posted on it?
- 2.4.2 What review process will ensure that company confidential information is not posted on the web site?
- 2.4.3 May employees communicate with customers, vendors, outside counsel or other persons via E-Mail (both internal and Internet varieties)?
- 2.4.4 What types of information will employees be prohibited to transmit via E-Mail? Will there be limitations, for example, on the E-Mail transmission of customer lists, pricing, contract terms and conditions or marketing plans? Will the company's in-house and outside lawyers be directed to use, or refrain from using, E-Mail for potentially privileged communications?

2.5 Employee Relations

- 2.5.1 May employees transmit personal messages via E-Mail?
- 2.5.2 How will employees be educated and warned regarding the potential for harassment claims arising from the inappropriate use of E-Mail?

2.5.3 Will employee computer stations be secured by access codes? Who will have access to those codes? May employees share their codes or disclose them to others? (Consider, for example, the executive who asks a secretary to review the executive's E-Mail while the executive is traveling).

2.5.4 May employees have dial-in access to the company network from off-premises?

CONCLUSION

The use of cyberspace in the workplace will require some getting used to, and over time everyone will become more familiar with it. However, in the interim, the pitfalls for an organization are real and it is accordingly important to address issues now, before serious problems arise. A clear policy will guide employees to make more efficient use of cyberspace technology and sensitize employees about the potential risks for their employers. A comprehensive cyberspace policy will also establish an understanding in the minds of senior management of the risks and rewards for the use of cyberspace and perhaps facilitate more effective management decision-making.

-
1. By "cyberspace" the authors refer to the place where online activities occur, either the Internet or a company's Intranet.
 2. Revised Statutes of Quebec (R.S.Q., c. C-12).
 3. Revised Statutes of Quebec (R.S.Q., c. S-2.1).
 4. Revised Statutes of Quebec (R.S.Q., c. P-39.1).
 5. "**Section 51.** Every employer must take the necessary measures to protect the health and ensure the safety and physical wellbeing of his worker. He must, in particular,
 - (1) see that the establishments under his authority are so equipped and laid out as to ensure the protection of the worker;
 - (2) ensure that the organization of the work and the working procedures and the techniques do not adversely affect the safety or health of the worker".
 6. "**Art. 35.** Every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law."
 7. "**Art. 36.** The following acts, in particular, may be considered as invasions of the privacy of a person:
 - (1) entering or taking anything in his dwelling;
 - (2) intentionally intercepting or using his private communications;
 - (3) appropriating or using his image or voice while he is in private premises;
 - (4) keeping his private life under observation by any means;
 - (5) using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
 - (6) using his correspondence, manuscripts or other personal documents."
 8. (1996) 22 C.C.E.L. (2d) 137 (B.C.S.C.).
 9. Canadian Railway Office of Arbitration, case no 2731, 14th of May 1996 (unreported).

10. Claude Lauzon, Arbitrator, July 24th, 1997 (unreported).

11. D.T.E. 94T-405 (C.T.).

12. In the province of Quebec, a Labour Commissioner is an administrative tribunal, comparable to a labour arbitration board, that hears statutory recourses from employees. Employees may seek such recourse against dismissals made without just and sufficient cause or against dismissals made for prohibited grounds such as pregnancy or illness.

13. Other decisions of interest include, the recent case of *R. vs. Pecciarich* (1995) 22 O.R. (3d) 748 (Ont. ct. prov. div.), where the accused was charged under the *Criminal Code* with unlawful distribution of obscene materials and unlawfully distributing child pornography in the form of computer images and text files. The files contained or were associated with a code name "Recent Zephyr". The Court used circumstantial evidence and admissions to find that the accused had unloaded obscene and pornographic images and texts onto bulletin boards under his code name of Recent Zephyr. The Court also addressed the issue of whether unloading images and text files onto a bulletin board constitutes "distribution" under Canadian Criminal Law.

In the case of *Canadian Catholic Organisation for Development and Peace vs. Union of employees for Development and Peace* (free translation) D.T.E. 97T702 (T.A.), an employee was dismissed after she had circulated, via E-Mail, a letter openly attacking her colleagues and management. The dismissal was reduced to a suspension on account of the employee's long years of service and because the arbitrator was of the opinion that the employer had acted in a discriminatory fashion by dismissing the employee when he had on a previous occasion only suspended an employee who had distributed similar material criticising management. Finally, in *Christensen v. ArmTec* (1996) 22 C.C.E.L. (2d) 225 (B.C.S.C.), an employee was summarily dismissed for *inter alia* circulating a memo criticizing the employer's president via E-Mail. The message was distributed to all of the employees in Western Canada. The Court found that the employer had sufficient grounds for dismissing the employee.

14. Burton Kainen and Shel D. Meyers, *Turning Off the Power on Employees: Using Employees' Surreptitious Tape-Recordings and E-Mail Intrusions in Pursuit of Employer Rights*, 27 *Stetson L. Rev.* 91 (Summer 1997); Jarrod J. White, *Email@Work.Com: Employer Monitoring of Employee E-Mail*, 48 *Ala. L. Rev.* 1079 (Spring 1997); John Araneo, *Pandora's (Email) Box: E-Mail Monitoring in the Workplace*, 14 *Hofstra Lab. L.J.* 338, at 345 (Fall 1996); Paul E. Hash and Christina M. Ibrahim, *E-Mail, Electronic Monitoring and Employee Privacy*, 37 *S. Tex. L. Rev.* 893 (June 1996); Laura B. Pincus and Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers*, 33 *Am. Bus. L.J.* 51 (Fall 1995); Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the «Electronic Sweatshop»*, 28 *John Marshall L. Rev.* 139 (1994); Note, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 *Am. U.L. Rev.* 219 (Fall 1994); Julia Turner Baumhart, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 *Lab. Law.* 923 (Fall 1992).

15. See *Playboy Enters Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) (display of copyrighted photographs on Internet bulletin board infringed rights of copyright owner); *Sega Enters. Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. Cal. 1994) (granting preliminary injunction and holding that uploading pirated video games to Internet bulletin board was one act of copying and that subsequent downloading of video games was an additional act of copying).

16. See *Telerate Sys. Inc. v. Caro*, 689 F. Supp. 221 (S.D.N.Y. 1988) (granting preliminary injunction and holding software developers liable for copyright infringement where developer's program allowed users to download database from private database service). See also *Shapiro, Bernstein & Co. v. Veltin*, 47 F. Supp. 648 (W.D. La. 1942) (holding proprietor of dance hall liable for infringing performances of copyrighted songs in dance hall by orchestra leader even though proprietor expressly directed orchestra leader not to perform infringing songs); *Swallow Turn Music v. Wilson*, 831 F. Supp. 575, 579 (E.D. Tex. 1993) (proprietor of tavern liable for copyright infringement by band notwithstanding contract between proprietor and band prohibiting infringing performances).

17. Sega Enters. Ltd. 857 F. Supp. at 686 (concluding that «unauthorized copies of these games are also made when they are downloaded»). See also MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993) (concluding that «'copying' for purposes of copyright law occurs when a computer program is transferred from a permanent storage device to a computer's RAM [random access memory]»).
18. For example, in Strauss v. Microsoft Corp., 814 F. Supp. 1186 S.D.N.Y. 1993), the court admitted evidence in a sex discrimination case of E-Mail communications by plaintiff's supervisor referring to one female employee as «Spandex Queen» and another female employee as «Sweet Georgia Brown» and referring to the plaintiff's supervisor as «President of the Amateur Gynecology Club».
19. Mitch Betts and Joseph Maglitta, *IS Policies Target E-Mail Harassment*, Computerworld, Feb 13, 1995, at 12.
20. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) (the «ECPA»).
21. 18 U.S.C. § 2511(2)(d) (1994).
22. 18 U.S.C. § 2510(5) (1994).
23. 18 U.S.C. § 2701 (1994), as amended.
24. See, e.g., Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (holding that alpha-numeric paging messages transmitted through system owned by employer were temporarily «stored» in computer before being transmitted to recipient's pager and indicating that electronically «stored» messages were subject to review by employer without having to rely upon the «consent» or other exceptions required to intercept communications under Title I of the ECPA. See also Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) (interpreting the legality of the seizure of messages from a bulletin board's physical computer server and distinguishing between the interception of messages under Title I of the ECPA, 18 U.S.C. §§ 2510 to 2521 (1994), as amended, and the seizure of stored messages under Title II of the ECPA, 18 U.S.C. §§ 2701 to 2711 (1994), as amended).
25. See, e.g., Cal. Penal Code § 632 (Supp. 1998).
26. No. BC007036 (Cal. Super. Ct. filed Mar. 12, 1991) *discussed in Electronic Mail Raises Issues About Privacy, Experts Say*, Daily Lab. Rep. (BNA) No. 222, at A-7 (Nov. 17, 1992)).
27. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).
28. Steven C. Kahn, Barbara Berish Broqwn and Michael Lanzarone, Legal Guide to Human Resources § 10.03[2][d] (1996).
29. Roboserve, Ltd. v. Tom's Foods, Inc., 940 F.2d 1441 (11th Cir. 1991) (trade secret elements of machines lost trade secret status when they were sold because «the sale destroyed any reasonable expectation of secrecy by placing the machines in the public domain»). See also Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 484, 94 S.Ct. 1879, 1887, 40 L.Ed.2d 315 (1974) («By definition, a trade secret has not been placed in the public domain»).
30. Religious Tech. Ctr. v. Lerma, 897 F. Supp. 260 E.D. Va. 1995) (documents not given trade secret status where court found they had been posted on Internet bulletin boards).
31. C. Geoffrey Weirich and James R. Glenister, *Revisiting Trade Secrets and Issues of Confidentiality in the Employment Context*, 1 Ga. B. J. 35, at 37 (June, 1996) (suggesting that «employers must institute as many safeguards as possible before employees abscond with information»). The quantity of safeguards necessary to maintain trade secret status is not absolute and will be determined on the basis of what is reasonable under the circumstances. See 1 Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.07[2] (1996). Merely requiring employees to sign confidentiality agreements may not be sufficient. See, e.g., Equifax Serv., Inc. v. Examination Serv., Inc. 216 Ga. App. 35, 453 S.E.2d 488 (1994) (declining to afford trade

secret protection to a list of customers and business partners where the company had signed confidentiality agreements with its employees but had not taken other reasonable steps to maintain the secrecy of the list).

32. Bert L. Slonim, *E-Mail and Privileged Communications: What are the Security Concerns?*, N.Y.L.J. (Nov. 24, 1997) (there are «no clear answers» to the question of whether attorney/client communications on the Internet create a waiver of the attorney/client privilege). Compare Freivogel, *Communicating With or About Clients on the Internet: Legal, Ethical and Liability Concerns*, ALAS Loss Prevention J. 17 (Jan. 1996) (concluding that «malpractice jurisprudence does not require that lawyers take extraordinary measures to prevent criminal interceptions [of Internet E-Mail]») with Iowa Bar Association Formal Opinion 96-1 (1996) (requiring, for purposes of legal ethics, that lawyers either obtain client consent before communicating by E-Mail or that lawyers encrypt E-Mail containing privileged material).

33. John Araneo, *Pandora's (Email) Box: E-Mail Monitoring in the Workplace*, 14 Hofstra Lab. L.J. 338, at 345 (Fall 1996) (costs of producing E-Mail in litigation is «a legitimate concern for any employer»). See also *In re Brand Name Prescription Drugs Antitrust Litig.*, No. 94 C 897, MDL 997, 1995 WL 360526, at *1 (N.D. Ill. June 15, 1995) (obligating employer to pay approximately \$60,000 to produce E-Mails subject to plaintiffs' discovery requests) *but cf.* *Bass Pub. Ltd. Co. v. Promus Cos.*, No. 92 Civ. 0969 (SWK), 1994 WL 702052, at *1 (S.D.N.Y. Dec. 15, 1994) (declining to order employer to produce E-Mail records for set of 100 employees but instead ordering the production only for a limited set of 10 employees).

Any inquiries of comments concerning this document should be addressed to Christopher Deehy at 514-925-6353.

This document is designed to provide information of a general nature only. It is not intended to provide legal advice and should not be acted upon without further consultation with professional advisors.