Executive Employment

a journal devoted to employment and related contract, dismissal and liability issues

Volume VII, No. 4 2000

Highlights

Board

Federated Press

WORKPLACE PRIVACY

Monitoring of Workers and Workplace Records in the Internet Age

Joe Conforti
Goodman Phillips & Vineberg

Introduction

The use of electronic communications within the workplace and externally has fundamentally changed the modern workplace.

Technological advances have created the ability to collect, store, process, retrieve and communicate enormous amounts of data in ways never before possible. Enhanced commercial opportunities are obvious. However, the proliferation in electronic communications and storage in the workplace is accompanied by the risk of access to private information – without the consent or even the awareness of the individual.

The potential conflict is evident: workers' expectations favouring individual privacy and restricted disclosure *versus* employers' needs to protect business interests, to monitor day-to-day operations, and to provide a safe, lawful and productive working environment. Balancing these interests will impact the future of the Canadian workplace.

Privacy versus Disclosure

Privacy is about *control* over workers' personal information: "the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself."[1]

Monitoring in the workplace includes: aural or visual surveillance (typically using closed-circuit television systems); telephone surveillance; computer-based monitoring (e.g., collecting performance data for employees working on computers from the time they log-on to log-off); e-mail and Internet tracking; access control systems (e.g., card keys and key pads measuring the time spent on-site); vehicle tracking (using transmitters or transponders).

Privacy, specifically related to access and monitoring of employee conduct, is not a new issue.[2] However, modern technology makes accessibility of records far easier and more cost-effective than ever before. Detection is often impossible.

Privacy advocates maintain that certain employment practices are highly intrusive and a threat to workplace privacy. Their concerns regarding electronic monitoring, employee testing and misuse of employment records relate largely to loss of personal autonomy, lack of consent to monitoring, testing or collection of personal information, and the potential that irrelevant personal information will be collected and disseminated. There is increasing concern that personal records maintained on databases can be sent across national borders, re-sold or integrated with other databases for purposes wholly unrelated to those for which the information was originally provided: "the data shadow cast by an individual in a series of transactions on the information highway can be assembled into a pattern which will allow a profile to be developed of an individual's lifestyle, personal habits, and buying power and preferences."[3]

Workers' concerns appear justified. American survey information demonstrates an alarmingly high rate of disclosure by large employers of private workplace information: 70% of employers surveyed disclosed workers' personal information to non-government creditors, with half of those workers not even being informed; this is compounded by the fact over one-third of employers do not even inform workers of the types of records maintained on them.[4]

[1] *R. v. Duarte*, [1990] 1 S.C.R. 30, at 46.

[2] See, e.g., Picher, "Truth, Lies and Videotape: Employee Surveillance at Arbitration" (1998), 6 *C.L.E.L.J.* 345.

[3] Canadian Federal Advisory Council on the Information Highway, *Final Report on Privacy and the Canadian Information Highway* (1995), http://info.ic.gc.ca.

[4] Linowes, "Many Companies Fail to Protect Confidential Employee Data," *Electronic Privacy Information Center* (April 22, 1996), http://www.epic.org/privacy/workplace/linowespr.html.

In contrast, employers justify the need for access to workers' information and/or monitoring with organizational requirements. Potential justifications for access and monitoring include:

- *Productivity*. Employers seek to curtail abuse and enhance productivity. Modern technology is not always for an employer's exclusive benefit. Surveys have found, on average, that workers spend 1.2 hours per day on e-mail; at least 30% spend more than 1.2 hours per day on the Internet of which 60% was "wasted" time.[5]
- *Harassment/Defamation*. Employers may be vicariously responsible for harassment or defamations using their computer networks. E-mail leaves an electronic trail and, depending upon system storage and retrieval capabilities, may constitute the "smoking gun" for future litigation.
- *Pornography*. Obscenity may expose employers to criminal charges. An employer will, therefore, need to ensure that its computer system not contribute to the proliferation of illegal materials.
- *Security*. E-mails sent on the Internet are not always secure. Information might be accessed by any intermediate computer between originator and recipient. Remote access and Internet connections increase the risk of maintaining trade secrets and makes employers vulnerable to virus attacks capable of destroying or altering valuable corporate data.
- *Software Piracy/Copyright Infringement*. Civil and criminal penalties for copyright infringements have increased in recent years. Improper use by workers of counterfeit or of copied software may be copyright infringement with substantial damages potentially accruing to the employer as well.
- *Workplace Investigations*. No investigation of just cause/discipline, harassment/discrimination, accidents or the like can be complete without accessing all relevant records, even if they are stored electronically.
- *Confidential and Proprietary Information*. Employers need to track and prevent unauthorized use of confidential, proprietary or other resources in the case of an unscrupulous departing worker using corporate resources for personal gain.

[5] Dichter, et al., "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age," *The American Employment Law Council, Fourth Annual Conference* (October 2, 1990).

Worker Records

In the workplace context, highly personal information is provided to employers by job applicants and workers during the course of employment. Generally speaking, when individuals disclose information about themselves, they do so for specific and limited reasons. This may be to obtain a benefit (including the job itself) or under legal compulsion. This includes:

- information necessary to obtain or continue employment (e.g., name, qualifications, education, previous employment, Social Insurance Number);
- information necessary to participate in group insurance, pension or other benefits (e.g., age, marital or family status, medical records);
- information concerning the worker's performance and conduct (e.g., performance appraisals, disciplinary record, etc.).

While individuals reveal much about themselves in the course of employment, they do not necessarily expect that the information will be subject to further public disclosure without consent.

Most jurisdictions have legislation protecting the confidentiality and limiting the use of personal information in the control of government;[6] however, there is no comprehensive legislation protecting workplace privacy within the private sector. The legislation that does exist is piece-meal, typically addressing privacy concerns only tangentially.

Recently, the Canadian government enacted Bill C-6, the *Personal Information Protection and Electronic Documents Act*,[7]

[6] See, e.g., *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. E-30 and *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

[7] Second Sess. 36th Parliament, S.C. 2000.

significantly broadening protection of personal information (including employee records) and, for the first time, imposing minimum obligations on the private sector. Initially, Bill C-6 will apply to the federally-regulated private sector only (including telecommunications, broadcasting, banking and inter-provincial transportation) as well as to designated Crown corporations and federal entities. In three years, Bill C-6 will apply to all personal information collected, used or disclosed "in the course of commercial activities" by all employers, when a province adopts legislation that provides substantially similar protection, those organizations covered by provincial legislation will be exempted from the federal legislation.

Bill C-6 is based on the Canadian Standard Association's Model Code and its "Ten Principles of Privacy":

1. *Accountability*. An employer is responsible for personal information under its control and shall designate an individual or individuals who are accountable for compliance. Accountability includes implementing procedures to protect personal information, procedures to receive and respond to complaints and inquiries, training and communication of staff.
2. *Identifying Purposes*. Purposes for which personal information is collected shall be identified by the employer at or before the time the information is collected.
3. *Consent*. The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
4. *Limiting Collection*. The collection of personal information shall be limited to that which is necessary for the identified purposes. Information shall be collected by fair and lawful means.
5. *Limiting Use, Disclosure and Retention*. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as is required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
6. *Accuracy*. Personal information shall be as accurate, complete and up-to-date as necessary for the purposes.
7. *Safeguards*. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Regardless of the format in which the personal information is held, protection against loss or theft as well as unauthorized access, disclosure, copying, use, or modification is required. Protection includes physical measures (e.g., locked file cabinets), organizational measures (e.g., limiting access to a "need-to-know" basis) and technological measures (e.g., passwords and/or encryption).
8. *Openness*. Employers shall make readily available to individuals specific information regarding its management of personal information.
9. *Individual Access*. On request, an individual shall be informed of the existence, use and disclosure of personal information about the individual and shall be given access to the information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. *Challenging Compliance*. An individual shall be able to address a challenge concerning compliance with the principles to the accountable individual. Employers shall investigate all complaints and, if justified, take appropriate measures.

The Federal Privacy Commissioner will have general powers to receive and investigate complaints and to attempt dispute resolution. The Federal Court will have authority to implement the appropriate remedies (including changes in practices, damages in compensation as well as for "humiliation").

Monitoring of E-Mail

Electronic monitoring is becoming easier and less expensive as new software can track web sites visited by workers and the time spent on each. Privacy concerns are heightened because this surreptitious surveillance can possibly monitor workers' conduct which does not necessarily affect the workplace and which may occur off-hours or even, in the case of remote access, off-site.

A recent American survey disclosed that almost two-thirds of the employers surveyed practice some form of electronic monitoring and surveillance.[8] Another survey showed that 22% of the employers sampled had searched their employees' computer files, e-mails or voicemail; significantly, 66% did so without the knowledge or consent of the workers concerned.[9]

Prior to embarking any electronic monitoring of workers, then, employers should be extremely careful to examine the rationale for monitoring as well as the method chosen to implement the process. Moreover, if the employer attempts to rely on the results of worker monitoring (e.g., to support or substantiate discipline or dismissal), there is an issue as to whether the results were properly obtained and, therefore, whether the results of the monitoring are admissible into evidence. Covertly obtained evidence is usually viewed as highly intrusive. In the context of governmental surveillance (i.e., police wire-taps), courts have imposed a high standard, saying "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance."[10] Therefore, such evidence may be of questionable admissibility during a legal proceeding. Even if an employer suspects that a worker engaged in illegal conduct, police assistance should be sought, in which case proper surveillance can be conducted pursuant to a judicially-approved warrant or wiretap.

Based on guidelines applicable in employee search and surveillance cases, the acceptability of e-mail or Internet monitoring will depend on a balancing of the employer's legitimate business interests with workers' expectations and right to privacy. The following factors will be relevant:

- Is the workplace unionized or non-unionized?
- If unionized, does the collective agreement address the issue?
- What is the purpose? Is it for productivity or to oversee the employees, or for security, safety or other overriding reasons?
- How was the monitoring carried out? Does it include off-site or off-hours surveillance?
- Are workers aware of the monitoring?

E-mails and the Internet operate over telephone lines. Any electronic monitoring should, therefore, respect all statutory provisions. It is a criminal offence to intercept a private communication:

> Everyone who by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.[11]

The *Telephone Act*[12] creates a separate provincial offence.

These provisions mean, in essence, that the act of recording or even listening to any oral conversation or telephone conversation (including voice-mail) is prohibited *unless* it would be unreasonable for the originator of the communication to expect that it would not be intercepted (i.e., the conversation or messages are clearly not private) *or* there is consent from at least one of the participants. Note that only the communication (i.e., the conversation itself) is considered "private" under the Criminal Code. The origin, destination or length of private telephone conversations are not private and, therefore, may be monitored.

Case Law

There is very little case law dealing with e-mails and the Internet. What little that exists tends to support the position that monitoring is permissible, primarily because there can be no reasonable expectation on the part of employees that e-mail or Internet communications are "private." See the following:

R. v. Weir:[13] In the course of repairing a customer's e-mail box, an Internet Service Provider recovered a message with child pornography attachments. The ISP informed

[8] American Management Association International, *1997 A.M.A. Survey: Electronic Monitoring & Surveillance*, http:\\www.amamet.org\survey\elec97.htm.
[9] Greenberg "E-Mail and Voice-Mail; Employee Privacy and the Federal Wire Tap Statute" (1994), 44 *The Am. U.L. Rev.*, 219, at 221-23.
[10] *R. v. Duarte*, supra note 1 at 43.
[11] Criminal Code, R.S.C. 1985, c. C-46, section 184(1).
[12] R.S.O. 1990, c. T.4, section 112.
[13] [1998] A.J. No. 155 (Q.B.).

the police and, at the request of the police, retrieved and copied the attachments. The Court was faced with the issue of whether the evidence was admissible. The Court reviewed the nature of Internet technology and concluded that: (i) access was readily available to anyone; (ii) the Internet system, being international, was not readily subject to legislation; and (iii) any transmitted messages passed through many Internet "nodes" and were subject to interception or interference at any point. In fact, the Court pointed out that "E-mail messages are easy to invade and a normal user would be none the wiser if invasion occurred." The Court concluded that e-mails did carry a reasonable expectation of privacy, but that this was a *reduced* expectation – at a level somewhat lower than first class mail or telephone conversations.

Smyth v. Pillsbury Co.:[14] In this case, the employer had assured workers that their e-mail communications would remain confidential. Nonetheless the employer fired an employee for sending inappropriate comments over its e-mail system. The Court dismissed the lawsuit, saying that it did 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." The Court determined that the employee lost any reasonable expectation of privacy by voluntarily communicating unprofessional comments over the e-mail. Finally, even if there was a reasonable expectation of privacy, the workers' actions were permitted as a matter of public policy:

> [W]e note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its E-mail system outweighs any privacy interest the employee may have in those comments.

Bourke v. Nissan Motor Corp.:[15] Two workers were discovered to be communicating personal messages containing sexually explicit content via the employer's e-mail system. The workers were issued written warnings for violating policy prohibiting the use of e-mail for personal purposes. As a result of continued protests by the workers, the employer discharged them. The workers sued for invasion of privacy and breach of criminal wiretapping and eavesdropping statutes. The Court affirmed judgment in favour of the employer, holding that the workers had no objective reasonable expectation of privacy in their e-mail messages. The workers each signed a waiver acknowledging the employer's policy restricting the use of e-mail for business purposes; the fact that the workers had been given private passwords to access the computer system did not create an irrebuttable privacy expectation. Finally, there was no improper wiretapping because the employer had every right to connect to the computer system as the system operator and did not access the workers' messages during transmission.

E-Mail/Internet Policy

It would be fair to say that, at the present time, employers are given substantial leeway in monitoring their workers' use of the Internet and e-mail.

As a precaution, in view of the Criminal Code, it would be prudent not to monitor nor to intercept any communications *while* any communications are in the process of being transmitted. Moreover, employers are in an even stronger position (and have far more certainty) if there is a written policy in place which obtains consent to monitoring, reduces any expectations of privacy, as well as defines the boundaries of proper conduct.

Any policy will depend on the business needs and human resources goals of the organization but would typically include certain components:

- A caution alerting employees that the e-mail/Internet system is for business use and that the employer retains the property rights in the system and all matters sent over the system or placed in its storage (including the absolute right to review, audit and disclose any such property in its sole discretion, with or without notice).

[14] 914 Supp. 97 (Ed. Pa., 1996).
[15] No. BO68705 (Cal. Ct. App., July 26, 1993).

- Confirm that the computer system should not be used to communicate any improper matters, e.g., discriminatory, derogatory, defamatory, obscene, or any otherwise unlawful or inappropriate materials.
- Provide a signed consent indicating its understanding of the company's policy.
- It would be useful to have an automatic reminder notice appearing on employees' computer screens when they log-in reminding them that e-mail on-line services may be monitored.
- Employees should be warned that deletion of any message or file may not fully eliminate it from the system and it will remain available for review.
- Confirm that violation may result in disciplinary action.

Conclusion

Modern technological advances have put individual workers' privacy rights on a potential collision course with their employers' access and monitoring of information.

A proactive approach would include the implementation of *both* privacy and monitoring policies which recognize the employer's legitimate interests, together with individual privacy interests.

While it is impossible to completely predict or safeguard from all risks, advance planning and open communications will minimize them.