

An Exploration of Workplace Privacy Issues In Canada

Richard S. Rosenberg, Professor Emeritus
Department of Computer Science
University of British Columbia

and

President, BC Freedom of Information and Privacy
Association and Board Member of BCCLA

Private Sector Privacy in a Changing World

PIPA Conference 2007

September 20, 2007

Vancouver, BC



*"We believe in employee privacy,
so keep your opinions to yourself."*

SOME SOURCES

- U.S. Congress, Office of Technology Assessment, *The Electronic Supervisor: New Technology, New Tensions*, OTA-CIT-333 (Washington, DC: U.S. Government Printing Office, September 1987).
- R. S. Rosenberg. *The Workplace on the Verge of the 21st Century*, *Journal of Business Ethics*, 22, 1999, pp. 3-14.
- V. Lockton and R. S. Rosenberg. RFID: The Next Serious Threat to Privacy. *Ethics and Information Technology*, Vol. 7, No. 4, December 2005, pp. 221-231.
- R. S. Rosenberg. The Technological Assault on Ethics in the Modern Workplace. In J. W. Budd and J. G. Scoville (Eds.) **The Ethics of Human Resources and Industrial Relations**. (Cornell, NY: Cornell University Press, 2005, pp. 141-171).
- V. Lockton and R. S. Rosenberg. A Preliminary Exploration of Workplace Privacy Issues in Canada. Office of the Privacy Commissioner of Canada Contributions Program, April 2006. <www.cs.ubc.ca/~lockton/workplace.pdf>

OUTLINE

- ▶ BACKGROUND
- ▶ US LEGAL PRECEDENTS
- ▶ SOME RELEVANT CANADIAN LAWS
- ▶ CURRENT AND FUTURE TECHNOLOGIES
 - RFID TECHNOLOGY
 - A GPS APPLICATION
- ▶ CONCLUSIONS (AND QUESTIONS)

BACKGROUND

- ▶ In 1987, the now defunct U.S. Office of Technology Assessment released a report, “The Electronic Supervisor: New Technology, New Tensions.”
- ▶ It describes a variety of technological threats to worker privacy.

Findings

- Computer technology makes possible the continuous collection and analysis of management information about work performance and equipment use.
- Computer-based systems offer opportunities for organizing work in new ways, as well as means of monitoring it more intensively.
- There is reason to believe that electronically monitoring the quantity or speed of work contributes to stress and stress-related illness ...

US LEGAL PRECEDENTS

- ▶ *Bonita P. Bourke et al. v. Nissan Motor Corporation (1993)*
 - The Court of Appeal upheld the original decision of the trial court in favor of the defendant, Nissan Motor Corporation in U.S.A. against the charge of the plaintiffs, “alleging wrongful termination, invasion of privacy and violation of their constitutional right to privacy in connection with Nissan's retrieval, printing and reading of E-mail messages authored by plaintiffs.”

Continued

- The trial court found in favor of Nissan on two grounds, of which the former is substantive: “Based on the undisputed facts, plaintiffs had no reasonable expectation of privacy in their e-mail messages.” Nissan presented additional arguments which have by now become familiar in the workplace, namely that only company business should be carried out on company computers and if warnings of lack of privacy are made generally available, workers have little to complain about.

Smyth v. Pillsbury (1996)

- This case has become exemplary in illustrating the power of management, even when an employee appears to be following company policy with respect to monitoring.
- Michael A. Smyth sued the Pillsbury Company for being wrongfully discharged, based on information obtained from Smyth's supposedly protected e-mail in spite of the fact that the company "repeatedly assured its employees, including plaintiff, that all e-mail communications would remain confidential and privileged. ..."

Continued

- “Defendant further assured its employees, including plaintiff, that e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand.”
- The judge found for the plaintiff and his reasons are revealing, particularly in the context of the accepted wisdom that well-defined and publicized e-mail policies are an absolute necessity for management to create an equitable and predictable environment. Consider the final paragraph of his decision:

Finally

- “In the second instance, 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.”

SOME RELEVANT CANADIAN LAWS

▶ PIPEDA

- This act applies to the collection, use and disclosure of information from commercial activities of any organization, as well the personal information of the employees of federally regulated private-sector organization.
- It does *not*, importantly, apply to employee personal information for provincially regulated businesses.

Two Particularly Relevant Clauses

- ▶ The first is section 5(3), which reads: “An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate under the circumstances.”
- ▶ Section 7(1)(b) reads: [An organization may collect personal information without the knowledge or consent of the individual only if] it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes relating to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

Implications

- ▶ Thus, employers subject to PIPEDA are allowed exceptions to ethical data collection principles if they are investigating a breach of contract (including the employment contract) or an illegal activity; when facing accusations of wrongful collection of personal information, companies frequently cite this exception.

Relevant Provincial Laws

- ▶ Personal Information Protection Acts of British Columbia and Alberta
 - PIPAs are not restricted to public works; they apply instead to “all organizations.”
 - Thus, companies in the private sector in both Alberta and BC cannot collect employee personal information without reason or justification; all the standards of reasonable collection, use and disclosure provided by PIPEDA for public sector employees are in force.

Continued

- An interesting clause in both PIPAs concerns the collection, use and disclosure, without consent, of employee personal data, essentially stating that consent is not required for reasonable collection of information, so long as notification is given, e.g. re Collection of employee personal information (in BC PIPA)
 - ▶ 13(1) Subject to subsection (2), an organization may collect employee personal information without the consent of the individual.
 - ▶ (2) An organization may not collect employee personal information without the consent of the individual unless
 - ...
 - ▶ (b) the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.

Continued

- ▶ (3) An organization must notify an individual that it will be collecting employee personal information about the individual and the purposes for the collection before the organization collects the personal information without the consent of the individual.
- Workplace privacy in Alberta and BC is thus held at lower importance than general individual privacy. While it is encouraging that notification was made mandatory, the fact remains that this clause weakens employee rights.

Quebec

- ▶ *Act Respecting the Protection of Personal Information in the Private Sector* (the Act is simply confirming rights set out in the *Civil Code of Quebec*, which in part reads as follows:
 - Chapter III – Respect of Reputation and Property
 - 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 unless authorized by law.
 - 36. The following acts, in particular, may be considered as invasions of the privacy of a person:
 - ...
 - 2) intentionally intercepting or using his personal communications;
 - ...
 - 4) keeping his private life under observation by any means;
 - ...
 - 6) using his correspondence, manuscripts or other personal documents.

Finally

- ▶ We can look at collective bargaining agreements in Quebec. For instance, an agreement between the *Journal de Montréal* and its unions requires that all surveillance be conducted with respect to the Quebec *Charter of Rights and Freedoms*.
 - [Kiss, S. and Mosco, V. (2005) "Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada", *Canadian Journal of Communications*, **30**, 549-564.]

CURRENT AND FUTURE TECHNOLOGIES

- telephone conversations are monitored,
- Web sites visited are logged and stored,
- e-mail messages are tracked and catalogued,
- Instant Messaging contributions are recorded,
- closed circuit television monitors are pervasive,
- active badges reveal workers' locations,
- as do global positioning devices embedded in cell phones,
- drug tests are performed randomly as well as scheduled,
- psychological tests are used to determine stability,
- genetic tests predict the possibility of terrible diseases,
- background checks are carried out prior to employment, and
- skills are gradually identified and extracted.

► RFID (Radio Frequency Identification) and GPS (Global Positioning Systems) technologies are on the move.

Current and Potential Future Uses of RFID Technology

- ▶ Animal tagging
 - Pets and Livestock
- ▶ Building access/quick payment fobs
- ▶ 40 million Americans already carry an RFID tag (as of 2004)
- ▶ Human Implants
- ▶ RFID-chipped Identification (e.g. Passports)

Implantable Chip Example

- ▶ A Cincinnati video surveillance company CityWatcher.com now requires employees to use VeriChip human implantable microchips to enter a secure data centre. Until now, the employees entered the data centre with a VeriChip housed in a heart-shaped plastic casing that hangs from their keychain.

<http://www.verichipcorp.com>

Finally

- ▶ The VeriChip is a glass encapsulated RFID tag that is injected into the triceps area of the arm to uniquely identify individuals. The tag can be read by radio waves from a few inches away.
- ▶ Implanting chips into humans in order to provide possibly tamper-proof identification is a serious step on the road to a massive violation of privacy rights.
 - Libbenga, Jan, Feb. 10, 2006. "Video Surveillance Outfit Chips Workers." *The Register*, February 10, 2006. Available at http://www.theregister.co.uk/2006/02/10/employees_chipped/

Global Positioning Systems

▶ Consider the following Headline:

- **Do you know where your workers are?**

GPS surveillance of employees can help efficiency, but raises privacy concerns.

Treena Hein, *The Globe and Mail*, January 18, 2007

Continued

- ▶ Ryan Vending, a Victoria-based company that fills and services vending machines throughout Vancouver Island and the Lower Mainland, wanted to know whether its drivers were receiving fair compensation for the hours and kilometres they logged on their delivery routes. So last fall, the company installed GPS devices into a portion of their 30-vehicle fleet and saw immediate benefits: The technology helped the company confirm its pay calculations were fair and balanced.
- ▶ Furthermore, Ryan Vending also discovered the technology improved their service-call response times, saved them money on fuel and stopped employees from abusing the privilege of taking company trucks home at night.

Finally

- ▶ Called telematics, the technology goes beyond simply providing businesses with vehicles' locations -- it can also supply data on things like when a vehicle's doors are open, when engines are turned on or when cargo has been picked up. What's more, the technology can also enable a business to remotely control a vehicle by turning off its engine, locking a door or disabling the ignition.

CONCLUSIONS

- ▶ “Continuous, indiscriminate surveillance of employees ... [is] based on a lack of trust and treats all individuals with suspicion, when the underlying problems may rest with a few individuals or with a management plan that may not be entirely sound. The effect of such omnipresent observation [is] stifling. ... The goal of ensuring adherence to the company’s vision comes at too high a price to our individual autonomy and freedom.”
 - Heather Black, Assistant Canadian Privacy Commission, 2004
- ▶ “With each new form of surveillance we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for ‘corrective’ measures.”
 - Bruce Phillips, (then) Canada Privacy Commissioner, 1993

Continued

- ▶ The legal environment currently favours the employer, as does the general balance of power within the workplace.
- ▶ People are more and more expected to do one of two things: work a mindless, de-humanizing position, or else define themselves by their job.
- ▶ Individuals in the former group are subject to continuous surveillance within the workplace in order to ensure that they do not deviate from the exacting specifications of their tasks, while their personal lives are thoroughly scrutinized to guarantee fitness for duty.

Continued

- ▶ Employees in the latter category are given more freedom to complete tasks as they best see fit, but are subject to intense monitoring to make sure that they not misusing time.
- ▶ They are also frequently expected to blur the line between on- and off-duty, as company resources are provided to allow for constant management or client accessibility. These are situations that should not be allowed to continue!
- ▶ Rules that effectively address an employer's right to monitor computer activity are based on the assumption that that computer is within the workplace; what happens when, as more and more frequently is occurring, that computer moves into the employee's home?

Finally

- ▶ What will employers be allowed to do when a simple medical test gives them access to a complete genetic profile? How can an individual complain about workplace monitoring when he or she cannot detect it, or when it is so commonplace that it is deemed 'reasonable'?
- ▶ These are but a few of the relevant questions with respect to workplace privacy, the answers to which will be vitally important in determining the extent to which Canadian law recognizes such a "right", and the legal weight given to it.