New Technologies in the Workplace: Privacy Issues

Ontario Human Resources Professionals Association
Ottawa,ON - October 23, 2007

Philippa Lawson, Director
Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
www.cippic.ca

Louisa Garib, LL.M.
Barrister & Solicitor
Ottawa, ON

cippic

Université d'Ottawa - University of Ottawa

Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Welcome to The Canadian Internet Policy and Public Interest Clinic

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established in fall of 2003 at the University of Ottawa, Faculty of Law, Common Law Section. CIPPIC seeks to ensure balance in policy and law-making processes on issues that arise as a result of new technologies. Clinic counsel work with upper year law students on projects and cases involving the intersection of law, technology and the public interest.

Read the latest **CIPPIC Bulletin**, published on August 27th, 2007

English Bulletin PDF
Bulletin Français PDF

Public Consultations

Public Safety Canada Consultation on Police Powers

The federal government is seeking comments on a proposal to force TSPs to hand over customer name and addresss information to police upon request, without reasonable grounds to suspect criminal activity. We have been informed that comments will be accepted until **October 19, 2007.**

ID Theft: Are you a victim?

CIPPIC is researching the phenomenon of identity theft with a view to making recommendations for policy and law reform. We are looking for victims of ID theft to assist us by completing a brief questionnaire and possibly a short telephone interview. If you are interested, please sen an e-mail to Mark Hecht, Senior Researcher at mhecht@cippic.ca.

Upcoming Events

The Revealed "I": A Conference on Privacy and Identity

October 26-27, 2007
University of Ottawa, Faculty of Law

CIPPIC News XML

CIPPIC critiques proposal for police access to subscriber data

New Technologies

- Video surveillance
- Email monitoring
- Internet use monitoring/restrictions
- Computer use monitoring
- GPS/location monitoring devices
- Drug/alcohol testing
- Biometrics
- Blogging; Personal webpages

Employer Uses

- Monitoring:
  - Protection against theft/fraud
  - Detecting/documenting misconduct
  - Ensuring conformity with laws/standards
  - Ensuring productivity
- Attendance Management
- Workplace Safety (drug/alcohol testing)
- Background Checks

Privacy Commissioners

- An employer's need for information should be balanced with an employee's right to privacy
  - privacy rights flow from contract, statutes/civil code, Charter of Rights, or common law
  - inherent right to privacy?

- Whether or not employee privacy is protected by law or contract, respecting privacy in the workplace makes good business sense

Arbitrators (majority)

"…as between employer and employee, the latter's *reasonable expectations of privacy* are not set aside simply by the entering into of the employment relationship; ...but just as an employee's privacy interests require protection against the overzealous exercise of management rights, so also must an arbitrator acknowledge the employer's legitimate business and property interests. What is required, then, is a contextual and reasonable balancing of interests. There is no absolute rule affording precedence to one legitimate interest over the other…."

Arbitrators (minority)

- no inherent right to privacy
  - must be based in contract or statute
- but employees may have privacy “interests” worth protecting
- key factor in analysing “breach of privacy” claims = employer’s duty to act fairly and reasonably

Applicable Law

- Contract/Collective Agreement
- Data Protection law
  - public sector statutes
  - private sector statutes
    - *PIPEDA*
    - *Alta PIPA, BC PIPA, Quebec Act*
    - Gap: employees of provincially-regulated private sector companies in other provinces
- Common law
  - nascent recognition of tort of “privacy invasion”
    - *Somwar v. McDonald’s* (Ont SCJ, 2006)

Public Sector - *Privacy Act*

- can collect, use, disclose employee information without consent if it relates directly to an operating program or activity of a public body
  + can disclose for variety of other specific listed purposes

Public Sector - *Charter*

- *Canadian Charter of Rights and Freedoms*
  - s.8: "Everyone has the right to be free from unreasonable search and seizure"
    - protects "reasonable expectations of privacy"
  - s.7: "Everyone has the right to life, liberty, and security of the person"

"….*grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection*…." (LaForest, J., *R. v. Dyment* (1988))

Private Sector - PIPEDA

- protects “personal information”
  = info about an identifiable individual, other than name/business contact info of employees
- no special rules for workplace
- must not collect, use or disclose PI without the individual’s knowledge and consent, or for inappropriate purposes
  – or in specific exceptional circumstances

Alberta/BC Approach

- “personal employee info” = personal info required & used solely for an employment relationship
- ERs may collect, use and disclose personal employee information without consent if the individual is an employee or potential employee AS LONG AS:
  - the collecting, using and disclosing of personal information is *reasonable for the purpose and limited to the work relationship*; and
  - *notice is given to employees* about the purpose for collecting their personal information.

Email Access/Monitoring

Email Access

- Employees have no reasonable expectation of privacy in email at work
  - *Camosun College v. CUPE* (Arb, 1999)
    - Email sent to Union members on ER computer network; was forwarded to management
  - *Briar et al v. Treasury Board* (PSSRB, 2003)
    - ER acting on complaint about offensive emails
    - ER had policy re: acceptable email use
    - Clear log-in warning that system is monitored for compliance with policy

Computer Surveillance

- Notice to employees is critical
  - written policy should be available to EEs
- Surreptitious monitoring of specific employee requires reasonable cause:
  - *Parkland Regional Library* (Alta IPC, 2005)
    - keystroke logging by ER
    - premature; less invasive means available

Video Surveillance

Hey boss. I'm not sure our covert surveillance is real covert any more.

Overt Video Surveillance

- *PIPEDA* #279:
  - webcams unjustified for monitoring employee productivity when managers off-site
  - “Continuous indiscriminate surveillance of employees was based on a lack of trust and treats all individuals with suspicion when the underlying problems rest with a few individuals or with a management plan that may not be entirely sound.”

Overt Video Surveillance

- *PIPEDA* #273:
  - webcams OK for purpose of protecting EEs of broadcasting company
    - no information collected
    - no reas. expectation of privacy in webcam locations
  - BUT must inform EEs & make policy document available to them

Overt Video Surveillance

- *Eastmond v. CPR* (2004) Fed Ct*:*
  - purposes = reduce vandalism, deter theft, reduce CP's liability for property damage, provide staff security
  - Test:
    - *Necessary to meet a specific business need?*
    - *Likely to be effective in meeting that need?*
    - *Is loss of privacy proportional to benefit gained?*
    - *Is there a less privacy-invasive means?*

Covert Video Surveillance

- higher threshold for acceptability:
  - – must be a substantial problem justifying surreptitious surveillance
  - + strong possibility that surveillance will be effective
  - + no reasonable alternative to surreptitious surveillance

Off-duty covert surveillance

- *PIPEDA* #269:
  - video surveillance to determine if EE truthful about physical limitations
  - need substantial evidence of broken trust + reasonable grounds to suspect violation of employment contract
  - no less invasive means available
  - OK in this case

GPS/Location Tracking

- *PIPEDA* #351:
  - should have clear policy on use of GPS so as to prevent “function creep” & to inform EEs
  - must notify employees up front
  - purposes must be appropriate
    - dispatch, asset management, safety OK
    - employee management OK in exceptional situations
  - no less invasive means of achieving purposes

Private blogs/publications

- *Chatham-Kent and CAW* (Arb, 2007):
  - careless public posting of personal info about clients +/or disrespectful comments about management can justify termination
- Corporate policies for employee blogging
  - limits to what employees are permitted to disclose
  - expectations regarding employee blogging
- Available to employers/potential employers
  - “publicly available” exception to consent requirement

Biometrics

Your DNA tests revealed that you are, in fact, a 93 year-old Chinese woman. I'm sorry, but since this job involves heavy lifting we cannot hire women or seniors.

Biometrics

- *IKO Industries Ltd. and U.S.W.A.,* (Arb, 2005)
  - hand scan = unreasonable privacy invasion
  - EE physical and informational privacy affected
  - balancing test: ER needs vs. EE rights
    - reasonable in circumstances
    - reasonable manner implemented
    - less intrusive, alternative means available

Biometrics

- *Canada Safeway Ltd. v. UFCWU (Arb, 2005)*
  - hand scan permissible
  - privacy intrusion minimal
  - balancing test: ER need > EE privacy loss
  - But concerned about:
    - lack of ER policies
    - destruction on termination
    - training and use of technology

Biometrics

- *Wansink v. Telus Communications Inc*. [2007] Fed CA (*PIPEDA* #281)
  - voice print used for authentication purposes
  - voice print = personal information
  - reasonable collection in circumstances
  - OK to discipline EEs who refuse
  - but ER not exempted from consent provisions
    - deficiency in PIPEDA?

Biometrics - summary

- Biometrics = Personal Information
- Reasonableness test applied
  - Does a problem exist? Can biometrics address it?
  - Is manner of implementation reasonable?
  - Alternative means explored?
- Notice (and consent) important
- Need policies for use, safeguarding, access, destruction
- Final thought: Religious accommodation? (407)

General Rules for Employers

- Don’t collect pi for inappropriate purposes
- Only collect what you need for stated purposes
- Always use least-invasive means
- Tell EEs what info you collect & why/how used
- Have a clear and complete policy on point
- Don’t engage in surreptitious surveillance without reasonable grounds/good justification (no other way of resolving problem)

www.cippic.ca