FEBRUARY 10, 2020

Smile! You're on Camera!

An Overview of the Law on Workplace Monitoring
Presented to CBA Privacy and Access Law North

Shannon Whyley
In-House Legal Counsel, Saskatchewan Teachers' Federation

SASKATCHEWAN TEACHERS' FEDERATION

Outline

I. Privacy Legislative Framework
   A. Public Sector
   B. Private Sector
II. Video Surveillance in the Workplace
III. Other Examples of Workplace Monitoring
   A. GPS Monitoring
   B. Workplace Computers
   C. Social Media
   D. Cell Phone Records
   E. Emerging Technologies

I. Privacy Legislative Framework

- Collection, use and disclosure of personal information of employees is regulated by different statutes.
- Personal information = Information about an identifiable individual.
  - Examples: name, sex, birth date, employment history, SIN, salary, religion, education, marital status, personal health information, etc.
- Collection of data about employees through electronic means (e.g., capturing images, movements, online activities) almost always involves collection of some level of personal information; therefore, privacy legislation matters.
- Different legislative considerations for public- and private-sector employers, and federally and provincially regulated employers.

A. Legislative Framework – Public Sector

- Both the provincial and federal jurisdictions have public sector privacy legislation governing employment information.
- Saskatchewan has the following statutes:
  - *The Freedom of Information and Protection of Privacy Act* (FOIP) for government institutions.
  - *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP) for local authorities.
  - *The Health Information Protection Act* (HIPA) for personal health information.

B. Legislative Framework – Private Sector

- Federal: *Personal Information Protection and Electronic Documents Act* (PIPEDA).
  - Applies to **federally regulated** employers with respect to employment information.
  - Does not apply to provincially regulated employers with respect to employment information.
  - Applies to all organizations (provincial and federal) with respect to "commercial activities."
  - Sets out rules regarding the use, collection and disclosure of "personal information."

B. Legislative Framework – Private Sector

- PIPEDA
  - Codifies 10 principles with respect to the collection, use and disclosure of personal information set out in a schedule to the Act.
  - Basic premise is to balance an individual's right to privacy regarding personal information with an organization's need to collect, use and disclose personal information for appropriate purposes.

B. Legislative Framework – Private Sector

- Saskatchewan: No equivalent provincial employment-related privacy legislation to date.
- Useful guidelines for Saskatchewan:
  - Employers are required to act reasonably when collecting personal information, conducting background checks, or vetting candidates for employment.
  - Reasonableness is dependent upon a number of factors, including: amount/type of information, purpose, intended use, disclosure and reasonable alternatives.

B. Legislative Framework – Private Sector

- *The Privacy Act* (Saskatchewan)
  - Creates a tort for a person to "willfully and without claim of right" violate the privacy of another person.
  - Rarely used.
  - Despite the lack of PIPEDA-equivalent legislation in Saskatchewan, it is arguable that some similar privacy obligations apply based on common-law principles (e.g., arbitration law in the unionized context).

II. Video Surveillance in the Workplace

- In *Eastmond v. Canadian Pacific Railway,* 2004 FC 852, the complaint was made pursuant to PIPEDA, and the federal court adopted a four-part test:
  1. Is camera surveillance and recording necessary to meet a specific need of the employer?
  2. Is camera surveillance and recording likely to be effective in meeting that need?
  3. Is the loss of privacy proportional to the benefit gained?
  4. Is there a less privacy-invasive way of achieving the same end?

II. Video Surveillance in the Workplace

- Arbitrators in other jurisdictions (BC, AB, SK) have adopted slightly different tests depending on the legislative scheme.
- Under all tests, the purpose of the cameras is important.
  - Deterrence of theft = acceptable (*Unisource Canada Inc. v. CEP*, *Local 433,* [2003] BCCAAA No. 309).
  - Monitoring of productivity = may be unacceptable (*Puretex Knitting Co. v. C.T.C.U.* (1979), 23 LAC (2d) 14).

II. Video Surveillance in the Workplace

- A higher standard for covert surveillance (*RWDSU Local 955 v. Leon's Manufacturing Co.* (2006), 153 LAC (4th) 155).
  - Requires employer to provide justification for why employees are not informed of surveillance.
- Form of surveillance and amount of information obtained should be as minimally intrusive as possible.

II. Video Surveillance in the Workplace

- Example of Saskatchewan arbitration case which explored these issues: *RWDSU Local 558 v. Coca-Cola Refreshments Canada Company* (Vancise, January 15, 2016, unreported).
  - Employer unilaterally and without notice or negotiation with the union installed 22 surveillance video cameras inside and outside its warehouse distribution centre.
  - Union filed a policy grievance, alleging a violation of the collective bargaining agreement and *The Saskatchewan Human Rights Code.*
  - Employer asserted it was entitled to install cameras in the workplace in furtherance of legitimate business interests, including security, safety of employees, protection of employees' property and to guard against money and product loss.

II. Video Surveillance in the Workplace

- Arbitrator Vancise considered the following issues:
  - Has the company breached the collective bargaining agreement by reason that the installation of the video cameras is an invasion of privacy and a fundamental change in the terms and conditions of employment?
  - Was there a legitimate security or business interest, which would justify the installation of the video surveillance equipment in the workplace?
  - Is the installation of the video surveillance system a breach of *The Privacy Act* or *The Saskatchewan Human Rights Code?*

II. Video Surveillance in the Workplace

- The employer's evidence:
  - Video surveillance would not be used to monitor employees' performance and would not be used for disciplinary purposes.
  - The system was meant to replace an outdated and ineffective security and inventory system which did not use cameras.
  - The implementation of the new system was in response, in part, to a number of incidents of theft and fraud, including one in which an out-of-scope supervisor had defrauded the company of $12,000 in cash and $47,000 worth of product.

II. Video Surveillance in the Workplace

- The union's evidence:
  - The system was installed without notice or negotiation with the union, although it was not done clandestinely and employees were aware.
  - There was a lot of anxiety among employees about the anticipated use of the cameras, driven in part by a supervisor who repeatedly stated that he could see what everyone was doing in the plant by watching the videos (which was actually not the case).

II. Video Surveillance in the Workplace

- Arbitrator found there was nothing in the collective bargaining agreement preventing the employer from installing cameras or from surveillance in the workplace.
- As to the question of a legitimate business interest, the arbitrator adopted the two-part test from *R.W.D.S.U., Local 955 v. Leon's Mfg. Co.* (2006), 153 LAC (4^{th}) 155 (Sask Arb):
    1. Was it reasonable, in all of the circumstances, to commence surveillance?
    2. Was the surveillance conducted in a reasonable manner?
- The arbitrator agreed that the threshold for determining the reasonableness of non-surreptitious surveillance is lower than that for surreptitious surveillance.

II. Video Surveillance in the Workplace

- The arbitrator found that the installation of a video surveillance system was reasonable in all the circumstances, including that there was a legitimate business interest based on evidence of prior security issues and thefts.
- However, the arbitrator recognized that a great deal of suspicion and anxiety surrounding the installation and use could have been avoided if the company had simply informed the union and employees of the intended installation, use and location of cameras in advance.

II. Video Surveillance in the Workplace

- Turning to the manner in which the surveillance was conducted, the arbitrator considered that all cameras were stationary and could not be manipulated or used to zoom into a specific area; they were all “fish-eye” cameras that targeted specific areas that presented a security interest (such as exits and cash areas), and did not operate continuously, but rather were activated by movement.
- The only persons who had access to the video surveillance footage were two out-of-scope employees.

II. Video Surveillance in the Workplace

- The union conceded that 12 of the 22 cameras were located in reasonable areas.
- The arbitrator found that those and another nine were reasonably located, subject to three of those being retargeted:
  - Camera at the cash-drop area to be retargeted to take images only of the cashier's window and not to capture images of employees entering or leaving the lunch room.
  - Cameras in the drivers' rooms to be retargeted to monitor cash and filling out of cash receipts, but not to monitor lockers.
  - Camera targeting an outside area to be repositioned to more closely target only the overhead door.

II. Video Surveillance in the Workplace

- The arbitrator found one camera out of the 22 to be unreasonable and to be removed:
  - Camera showing the time clock – the arbitrator rejected the employer's concerns regarding need to guard against potential time theft and ruled it would add nothing to the company's security.
- As to the final issue, the arbitrator found it was not necessary to deal with the issue of whether or not *The Privacy Act* was contravened, since virtually all of the cameras were used in a reasonable manner and that there was no violation of *The Saskatchewan Human Rights Code.*
- Take-away from this case – the importance of evidence of legitimate business needs and reasonableness of implementation and use of technology to address those needs.

II. Video Surveillance in the Workplace

- What about video surveillance outside the workplace?
- This may be allowed where it occurs in a public place and while employees are actively engaged in a public activity:
  - *Amalgamated Transit Union Local No. 569 v. Edmonton (City)*, 2004 ABQB 280 – Employee videotaped while performing strenuous physical tasks while on disability leave.

II. Video Surveillance in the Workplace

- Contrast with the situation where surveillance evidence was ruled to be inadmissible because the employer did not have a reasonable basis to conduct surveillance (failed to properly investigate first) and failed to conduct the search in a reasonable manner (entered the employee's vacant home):
  - *Prince Albert Co-operative Assn. Ltd. And RWDSU, Local 496*, 2016 CarswellSask 282

III. Other Examples of Workplace Monitoring

- Technology has dramatically changed since the earliest cases of workplace monitoring through video surveillance (1970s).
- Arbitrators and courts attempt to seek a balance between employees' reasonable expectations of privacy and employers' legitimate business needs.

A. GPS Monitoring

- Several rulings from BC's Privacy Commissioner pursuant to BC's PIPA:
  - *Schindler Elevator Corporation,* 2012 BCIPC 25:
    - Elevator company employees stored vehicles at their homes.
    - Vehicles equipped with GPS tracking system that was only monitored by employer when an "exceptional use" report was generated.
    - BC Privacy Commissioner held that installation of GPS monitoring was "reasonable."
    - Factors include: sensitivity of employee personal information; amount of personal information collected; likelihood of effectiveness; manner of collection; and whether less-intrusive alternatives available.

A. GPS Monitoring

- Notably, the BC Privacy Commissioner rejected the four-part test applied under PIPEDA (as applied in *Eastmond*) for use in determination of complaints under PIPA.
- Decision followed in *ThyssenKrupp Elevator (Canada) Limited,* 2013 BCIPC 24 and *Kone Inc (Re),* 2012 BCIPC 23 (both in BC and both involving elevator companies too).

B. Workplace Computers

- *R. v. Cole*, 2012 SCC 53:
  - High school teacher's laptop contained nude photographs of minor student.
  - Evidence collected from the laptop *by* police violated Cole's *Charter* right to be free from unreasonable search and seizure.
  - Canadians have a reasonable expectation of privacy in their work computers where personal use is permitted or reasonably expected.
- *Charter* case determined in criminal law context regarding individual's right to be free from unreasonable search and seizure.
- Has been applied in labour decisions since.

B. Workplace Computers

- *R. v. Cole* – Reasonable expectation of privacy can be diminished by appropriately implemented workplace policy:
  - "While workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the expectation entirely: the nature of the information at stake exposes the likes, interests, thoughts, activities, ideas, and searches for information of the individual user."

B. Workplace Computers

- Reasonable expectation of privacy over workplace computers may depend on:
  - Whether the employee owns the hardware and/or software.
  - Whether the technology is being used during business hours.
  - The employer's policies surrounding Internet and email use.
  - Whether the employee has been made aware of the employer's policies.
  - The extent to which the employer's policies are regulated and consistently enforced.

C. Social Media

- Growing body of case law where employers have successfully disciplined for inappropriate social media use. Examples include:
  - *Saskatchewan Government and General Employees' Union v. Saskatchewan,* 2009 CarswellSask 913 (re: private Facebook group with racist theme and postings).
  - *Lougheed Imports Ltd. (cob West Coast Mazda*), [2010] BCLRBD No. 190 (re: posts insulting to employer and supervisors).
  - *Canada Post Corp and CUPW*, [2012] AWLD 2981 (Alta Arb) (re: derogatory and hateful posts about supervisor over a one month period).
  - *USWA, Local 9548 and Tenaris Algoma Inc.*, 2014 CanLII 26445 (ON LA) (re: harassing comments posted about coworker).

C. Social Media

- Some factors to be considered before issuing discipline for social media use:
  - Is there a real and material connection to the workplace, justifying discipline for off-duty conduct?
  - How serious is the incident?
  - How “private” is the information (e.g., private group chat vs. 400 Facebook friends)?
  - Does the employer have a social media use policy in place?
  - Are employees made aware of expectations surrounding appropriate social media use?
  - Does the employee hold a public role or position with an elevated level of trust?

D. Cell Phone Records

- *Canadian Railway Company v. Teamsters Canada Rail Conference*, CROA & DR 2900:
  - Employer requested copies of an employee's cell phone records as part of an investigation into a train accident.
  - Held: personal communications are, by definition, generally entirely unrelated to an employee's duties and responsibilities; however, an exception was found in this case for several reasons:
    - Information received only indicated that the employee had been making a call at a certain time; the phone number and content of any text was blacked out.
    - Employer chose the least-intrusive method of obtaining information.
    - Employer had a carefully drafted policy which respected the privacy rights of the employee.

D. Cell Phone Records

- Additional considerations:
  - Whose device is it?
  - What is the policy on use of personal cell phones during work?
  - What is the purpose for reviewing cell phone data?
    - E.g., investigating workplace accident vs. productivity concerns.
  - Differences in requesting limited data (e.g., log of incoming and outgoing calls, screenshots of selected text messages) vs. searching the device itself.
  - Are there less-intrusive ways of obtaining the same information?

E. Emerging Technologies

- Other types of data collection are emerging all the time as a result of evolving technology.
- Examples:
  - Fatigue/health-monitoring systems – headband, Fitbit.
  - Facial-recognition technology.
  - Other examples?
- Courts and arbitrators are likely to apply established principles around employee privacy to new technologies, while recognizing the new realities of the digital world.

E. Emerging Technologies

- General trends:
  - Any type of monitoring should be reasonably connected to the employer's business or management purposes.
  - Should be reviewed for compliance with legislation, collective agreements and employer policy before implementation.
  - Employees should be made aware of monitoring programs, reasons for them, and what information is being collected before the program is implemented.

Questions