Employee Privacy Rights in the Workplace

Privacy Law and the
Contemporary Workplace: New Challenges and Directions

Toronto, Canada, November 22, 2013

Faculty of Law Center for Law in the Contemporary Workplace – Queen's University

Leo McGrady QC and Maria Koroneos*

1. Introduction

One of the pleasures of being invited to speak on panels such as this, in addition to the company of my co-panelists, is having some of my own long-fixed ideas about issues effectively shredded by what I learn researching and also speaking with colleagues who are truly experts on the issues[1].

I began that process in this case with the notion that our attitude towards privacy as a community was relatively homogenous - that it was an important value deserving of our protection, and that was acutely so in the workplace where employees have perhaps the least autonomy. Here is some of what I discovered:

- At least one employer valued the contents of its vending machines in its lunchroom more than its employees' privacy when it argued that protecting these machines was sufficient justification for video surveillance. My office colleagues, assuming like most vending machines, this one dispensed twinkies, have come to refer to this as the company's twinkie defence[2].

---

* Lawyers with McGrady and Company, Vancouver BC. We would like to thank Kavita Goldsmith, a legal assistant in our office, for her invaluable assistance with the paper.

[1] Leo McGrady, *National Labour and Administrative Law CLE Conference: Pushing the Boundaries: Standing, Privacy and Practical Issues*, (Ottawa, Ontario, 21 November 2003), online: McGrady & Company <http://www.mcgradylaw.ca/Publications/Pushing_the_Boundaries.htm>; Leo McGrady, *Privacy Law Update*, Employment Law Conference 2004 (Continuing Legal Education) (Vancouver B.C. 24 April 2004), online: McGrady & Company <http://www.mcgradylaw.ca/Publications/Privacy_Update.htm>; Leo McGrady, Maria Koroneos & Janet Lennox, *When Privacy Interests Clash with Surveillance and Testing*, INSIGHT, Western Region Labour Relations (Vancouver B.C. 24 February 2004), online: McGrady & Company <http://www.mcgradylaw.ca/Publications/When_Privacy_Interests_Clash.htm>.

[2] *Cascade Aerospace, Inc. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 114*, [2009] CLAD No. 95, 186 LAC (4th) 26.

- That phrase became a password for 'junk law' theories, after the mythical defence supposedly raised in the 1979 San Francisco trial over the tragic murder of Harvey Milk. The person convicted, Dan White, was said to have argued the murder resulted from excessive consumption of sugar-laden twinkies[3].

- The most intensive workplace [at least nongovernmental] surveillance is by unionised employees - surveillance operators - of unionised employees - in a casino. The surveillance equipment consist of numerous video cameras that continuously feed live images of virtually all areas of the casino inside and outside to monitors inside the surveillance room. Most cameras have panel, tilt, and zoom capability and are operated remotely. Virtually every movement by every employee throughout his or her work day can be captured and recorded. Only those in the surveillance department know which cameras are in operation at any given time and what each camera's position is[4].

- Kathleen Miller in Bloomberg News, reports that the US is investigating whether it can scour social media websites used by employees as a way of assessing security and other risks from workers such as Edward Snowden and the Washington Navy Yard shooter[5].

- We were told that many younger employees view privacy concerns as a fixation of those over 50, who they view as a pre-facebook/twitter generation, raised on handwritten letters delivered by uniformed 'Post Office' personnel, and for whom cell phones were a novelty.

- Some have expressed the view that a partial answer to the inequity in privacy that exists is to monetize personal information that would have the effect of enabling people to control their own data and choose their own level of privacy. One consequence would be that data would become too expensive for businesses and governments to hoard and mine indiscriminately as they are doing now[6].

- The US Director of National Intelligence, James Clapper, has told us that despite recent disclosures of the extravagant range of operation of his agency, stripping organizations, individuals and countries of privacy rights, and doing so in complete "anonymity, secrecy, and darkness", that he "cares just as much about privacy and rights as the rest of us." He admits of no irony of course[7].

---

[3] Carol Pogash, (2003-11-23). "*Myth of the Twinkie defense*", San Francisco Chronicle. p. D-1 (accessed November 14, 2013).

[4] *Gateway Casinos and Entertainment Inc. v. COPE Local 378*, 2009 CanLII 59118, paras 7 – 11.

[5] Kathleen Miller, "U.S. Weighs Social-Media Searches for Clues to Rogue Workers", Bloomberg (31 October 2013) online:<http://www.bloomberg.com/news/2013-10-31/u-s-weighs-social-media-searches-for-clues-to-rogue-workers.html>

[6] J. Lanier, *How Should We Think About Privacy?* [2013] 309 Scientific American, Number 5, page 65.

[7] Natasha Hassan, "Is Edward Snowden a Hero", *Globe and Mail* (9 November 2013) page F9.

- Privacy is a core Western democratic value[7].

- Both the US National Security Agency (NSA) and the Communications Security Establishment Canada (CSEC) have the potential to create sophisticated maps of an individual's personal information in social connections. They also have the ability to sift through an immense amount of communications, data and zero in on the phones and computer servers that they determine merit attention[8].

- Occupy here is a private messaging forum developed at the same time as the Occupy movement several years ago. Each Occupy.here router is "a LAN island in an archipelago of affiliated websites". It offers a network of virtual spaces where both committed activists and casual supporters can communicate. Occupy.here is resistant to internet surveillance because of its distributed and autonomous design. Building up a collective network infrastructure that is owned and controlled by its users can lay the groundwork for other uses and applications[9].

- On October 22, 2013, the British Columbia Civil Liberties Association filed a claim in B.C. Supreme Court challenging for the first time CSEC's unmonitored practice of reading Canadians emails and text messages, as well as listening to their telephone calls when they communicate with someone outside the country. Most countries provide for a measure of this kind of secret activity. However, Canada is unique in that it provides for no meaningful oversight. Nor does it require the kind of safeguards that protect us from domestic spying by police agencies such as CSIS or the RCMP that, by law, are required to have a judicial warrant before intercepting the communications of Canadians[10].

- The number of drones being utilized by domestic police forces has increased dramatically in the past year, as has the range of purposes for which they are used. That is so despite the complete lack of oversight with respect to privacy issues and the ease with which they can be hacked. There are no reports of their utilization in employment settings, but given the rapid adaptation and utilization of parallel technology such as GPS, employment, utilization is not likely far off. Trucking, shipping, and rail are three that have been identified as likely prospects[11].

What I concluded from this research and these exchanges with my colleagues was markedly different than the notion I began with. Far from a relatively homogeneous approach to privacy

---

[8] J. Wortham, "Seeking Online Refuge From Spying Eyes", *The New York Times*, (20 October 2013) page 3; and C. Freeze and S. Nolen "Slides reveal Canada's powerful espionage tool", *The Globe and Mail* (19 October 2013) page A4.

[9] Occupy.here <http://occupyhere.org/>

[10] British Columbia Civil Liberties Association v The Attorney General of Canada, (22 October 2013) Reproduced on BC Civil Liberties Association website online:<http://bccla.org/news/2013/10/spying-in-canada-civil-liberties-watchdog-sues-surveillance-agency-over-illegal-spying-on-canadians/>

[11] K. Wesson and T. Humphreys, "Hacking Drones", [2013] Scientific American 309, number 5, page 55.

there is a dramatic range of views on its importance amongst employees. They range from the view that privacy is a self-indulgence on the part of over-50 Canadians, to the view that as a society we must have significant protection for privacy rights from employers, other commercial interests, and from government, to the notion that it is a core democratic value that must be protected at all costs.

One conclusion on which I believe everyone would agree is this, however, you may value or not value privacy rights, they are in tatters as a result of unmonitored and unregulated intrusions from commercial interests and from the government.

What I propose to do now is to review privacy rights in a range of employment settings and examine how they have been treated by arbitrators in that setting.

2. Video Surveillance - Real Time Monitoring

One of the most important decisions in this area is *Metso Minerals Canada Inc. v United Steelworkers*[12]. I include this case for its treatment of the employer's obligation to provide details and justification with respect to video surveillance installation.

Specifically, the employer had not provided sufficient information regarding the following factors in order for the union to assess the legality of the employer's intentions:

- the camera field;
- the use to which the surveillance would be put;
- that the first 3 cameras would be followed by 13 more;
- it had not been made aware of their placement;
- it was not aware that a manager would be able to real time the monitor the video feed from his laptop in Florida; and
- it may not have been aware that the employer may use the surveillance for disciplinary purposes.

Similar although less dramatic issues arose in *Cascade Aerospace, Inc. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 114*[13]. Cascade Aerospace was in the business of repairing and maintaining aircraft, both civilian and military. Its facility is at the Abbotsford International Airport. The company has a contract with the Department of National Defense, and there was no question that the workplace was safety sensitive - there was expensive material on site, as well as access to airport runway and to airplanes.

There were a number of cameras outside the building which the union did not dispute. However, when a camera was installed inside in the building, in the cafeteria - lunchroom, the union complained that this was contrary to federal personal privacy legislation (PIPEDA). The lunchroom was used by employees, contractors and visitors. The camera was installed to protect

---

[12] *Metso Minerals Canada Inc. v United Steelworkers (Workplace Video Surveillance Grievance)*, [2009] OLAA No. 508.

[13] *Cascade Aerospace, Inc. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 114*, [2009] CLAD No. 95, 186 LAC (4th) 26.

the cafeteria vending machines, however, the angle of the video coverage was wide enough to include several tables at which employees took breaks and ate their lunch. The arbitrator found that there was a breach of the legislation and by its carelessness in installing the camera at this particular angle the company exceeded its management rights.

3. Video Surveillance - the Test for Admissibility in Arbitration Proceedings

One of the hand full of leading cases on this issue is a Saskatchewan decision, *United Steelworkers, Local 7552 v Agrium*[14], which reviewed the various tests for admissibility of video surveillance in arbitration proceedings. It includes a discussion of the "reasonableness test", the "modified reasonableness test" and the "admissible in a court of law test". The case involved surreptitious video surveillance of an employee off work on worker's compensation.

> The Board began with the three point reasonableness test set out by Arbitrator Vickers in the British Columbia decision *Doman Forest Products Ltd. and I.W.A., Loc. I-357* (1990)[15]:
>
> (1) was it reasonable, in all of the circumstances, to request surveillance?
> (2) was the surveillance conducted in a reasonable manner?
> (3) were other alternatives open to the company to obtain the evidence it sought?

He then reviewed the modified reasonableness test which deleted the requirement for the employer to exhaust all other alternatives in obtaining the evidence before resorting to video surveillance. For this test, he adopted the reasoning of the Board in *Toronto Transit Commission and ATU Local 113*[16]:

> It is our view that it is not appropriate to include as a separate third aspect of any test a specific requirement that the employer must have exhausted all other alternatives before turning to video surveillance. Such a requirement puts too onerous a burden upon the employer and may not be appropriate in every case. It is important to look at the reasons why the employer chose to engage in surveillance and to determine in the specific circumstances of each case whether or not the decision was a reasonable one.

Finally he provided his assessment of the 3rd test, whether the video surveillance evidence was admissible in a court of law, a proposition he rejects. He then concludes:

> **54** …. Video surveillance of an employee's off-site activities should not be condoned when there is no reasonable basis to conduct the surveillance. Arbitrary or random surveillance runs afoul the purpose of the Collective Agreement. Such surveillance would not promote or continue the existing harmonious relations of the parties….
>
> **55** In my view, in the circumstances, the test the Employer must meet is to establish that it was reasonable to engage in the video surveillance and that the surveillance was conducted in a reasonable manner. I am of the view that it was reasonable in the circumstances for the Employer to request the video surveillance. In addition to Arnsten's direct observation of Schulte cutting the tall grass, there was chatter in the workplace that Schulte was building a house on the same acreage where he was seen cutting grass and the inquiry of another employee

[14] *United Steelworkers, Local 7552 v Agrium*, [2009] SLAA No. 9, 185 LAC (4th) 296
[15] *Doman Forest Products Ltd. and I.W.A., Loc. I-357* (1990), 13 LAC (4th) 275, pp. 281-282
[16] *Toronto Transit Commission and ATU Local 113*, (1999), 80 L.A.C. (4th) 53, at p 68-69

> as to how he could get on the same program of going off work to build a house while receiving Workers' Compensation Benefits. Not only is it reasonable for the Employer to want to get to the truth of the matter, it would be unacceptable for the Employer to put its head in the sand and do nothing with this information. As stated earlier, the second part of the test is conceded.
>
> **56** In my view it was not necessary, in the circumstances, for the Employer to exhaust all other alternatives before resorting to covert video surveillance to get the evidence it sought.

4. Video Surveillance - Public Place

Different considerations of course apply where the video surveillance is taking place in a public location. This point was made most forcefully in a federal privacy: *PIPEDA Case Summary #2009-001*[17].

The complaint was launched by an employee against his employer, an intercity bus company, using video cameras in a city bus depot to monitor and manage employee performance. The Privacy Commissioner found that the employer's stated purpose for the video surveillance did not involve employee monitoring, but rather the cameras were installed for the following purposes: to ensure the safety and security expectations of customers and employees; reduce and discourage incidence of vandalism and illegal conduct; and limit the potential for liability for damages due to fraud, theft or inappropriate operational procedures (i.e. accidents).

The 31 video cameras were not located in areas such as public washrooms or employee break rooms; however, they were located in employee workplace areas where the employer believed there was a concern for safety and security (movement of vehicles, freight and passengers), as well as in areas where there was a large amount of cash and freight handling.

The Commissioner accepted that it was not the employer's intention to use the video surveillance system to monitor employee productivity and accepted the employer's position that there was an assumption of consent for video surveillance for its use in the depot. It analogized the situation to clearly visible video surveillance cameras being located at the airport. The commissioner found that implied consent is a reasonable assumption for transportation facilities such as this bus depot. Further, there were signs and notices posted at all entrances and work areas advising of video surveillance.

Ultimately, the Commissioner recommended that the employer finalize its video surveillance policy and security personnel procedures (which were still in draft), train its security personnel and managers and establish guidelines for assessing compliance with the policy.

5. Video Surveillance - Public Places in Ontario

I include this case, *Windsor Essex County Health Unit v Canadian Union of Public Employees, Local 543*[18], in my paper for its discussion with respect to the grievor's privacy rights in a public

---

[17] *PIPEDA Case Summary #2009-001*, [2009] CPCSF No. 1

[18] *Windsor Essex County Health Unit v Canadian Union of Public Employees, Local 543*, [2011] OLAA No. 255, 208 LAC (4th) 392

place specifically in Ontario, which unlike British Columbia and Alberta, has no provincial privacy legislation.

Three public health inspectors were dismissed, based on covert surveillance and video recordings. The union argued for the "reasonableness test" for admissibility of the evidence. The employer argued that "relevance was the appropriate test", based on the absence of privacy laws in Ontario. The arbitrator found that the grievors did not enjoy a right to privacy in public places during working hours that would prevent them from having their presence or activities be observed, monitored, documented, photographed, or video recorded by the employer. Further, the employer can seek to introduce material of this nature into evidence without needing to demonstrate in evidence that it had reasonable grounds for undertaking the surveillance in the first place. The arbitrator's discussion of the jurisprudence with respect to privacy rights for an employee in Ontario follows below:

> **18** I find that on the basis of the cases placed before me and the submissions of the union, I am not persuaded that there exists in Ontario a general right to privacy such that it would preclude the observing of a person's presence or activities in public, the documentation of such presence or activities, or the photographing or video recording of such presence or activities. Neither am I able to find that there exists a general expectation of such a privacy right in public places in Ontario. Nor, in the matter of the instant case am I able to find that the collective agreement between the parties contains language that would preclude the employer from observing, documenting, photographing, or video recording an employee's presence or activities in a public place, or that would preclude the employer from monitoring an employee's work activities during working hours. Indeed in this general regard it is noted that the parties have in their collective agreement, in the Letter of Understanding at page 39, turned their minds to the matter of the monitoring during working hours of employees who have employer-issued Blackberry cell phones equipped with GPS Tracking. The agreement is not that employees cannot be monitored during working hours. It is that such employees are required to keep the GPS Tracking program active during all work hours, except lunch and breaks, and that the employer will not introduce evidence of GPS Tracking for the purpose of disciplining employees for work performance issues. I must conclude that this arrangement reflects a general understanding between the parties that employees can be monitored during working hours.

Some of the deficiencies complained of by employees in Ontario with respect to privacy issues may now be addressed as a result of the recent decision of the Supreme Court of Canada in *R v Cole*[19]. While the narrow focus of the court's findings related to the warrantless search of an employee's employer–owned computer by a police officer, the court also confirmed that employees do have a reasonable expectation of privacy with respect to information stored on workplace computers.

6. Video Surveillance - Workplace Safety and Food Safety

I have included these two issues together because they attract a similar analysis. The issue of the use of video surveillance for workplace safety purposes was the focus of this recent important

[19] *R v Cole*, 2012 SCC 53

decision from Manitoba: *New Flyer Industries Ltd. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 3003*[20].

New Flyer Industries installed cameras inside its paint shop, on the basis that the cameras were installed for health and safety reasons as well as for the protection of property. It also acknowledged that the video surveillance would be used for discipline. The union objected to the cameras, seeking a blanket prohibition, arguing that the surveillance was unduly intrusive and did not effectively address the objectives of the employer – that is they were not really helpful with respect to the safety of employees. The arbitrator found that the video surveillance was reasonable and that there was no need for a blanket prohibition.

Also at issue in this case was the question of "real time" surveillance:

> **74** The authorities reveal a recurring theme whereby unions worry about employers moving toward real time monitoring which may be used to scrutinize employee efficiency, production and attendance at individual work stations. The fear is that surveillance will be used to exert pressure and impose discipline when employees fail to meet operational demands. The present grievance raises this concern, alleging that the stated use of cameras for safety has evolved to a broader use including discipline.

In this case, it was agreed that supervisors could not view live or stored video without human resources authorization and accompaniment.

Similar concerns were raised in the leading case over food safety, with similar results: *Cargill Foods, a Division of Cargill Ltd. v United Food and Commercial Workers International Union, Local 633*[21].

At issue was Cargill's installation of video surveillance cameras in one of its large meat packaging plants. The union raised the issue of the use of video surveillance for disciplinary purposes. "Real time" surveillance was also again a concern. The union argued that the purpose of the additional cameras that were installed in the production area and hallways was to monitor employee conduct and to control time away from workstations - thereby substituting cameras for supervisors.

The arbitrator found that the primary purpose of the cameras in the production area was to support the food safety function. Food safety was clearly a legitimate management function. The arbitrator found that the video surveillance system had not been used to collect information about employees or identify situations for discipline. It had been used as an aid to investigate specific incidents. Further, the use of the surveillance system to investigate incidents relating to food safety, plant security and industrial discipline is a legitimate exercise of management rights. This finding was predicated on the employer's position that it does not use the video surveillance system to monitor employees in real time or otherwise.

---

[20] *New Flyer Industries Ltd. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 3003*, [2011] MGAD No. 27

[21] *Cargill Foods, a Division of Cargill Ltd. v United Food and Commercial Workers International Union, Local 633*, [2008] OLAA No. 393 and 2009 OLAA No. 633

In a follow up award, 2009 OLAA No. 633, the arbitrator set out a helpful protocol for the use of video surveillance:

> **3** Having regard to the parties' submissions and to the remedial considerations set out in the July 4, 2008, award, I award the following protocol for the use of the video surveillance system and its product, and direct the Employer to implement it in the workplace:
>
> 1. The Employer shall not use the video surveillance system to monitor employees, in real time or otherwise.
>
> 2. Recordings made by the video surveillance system shall be retained for no longer than six (6) months, except in the circumstances set out in the following paragraph.
>
> 3. When an incident or investigation occurs requiring the retention of video surveillance recordings, the Employer may retain those recordings for as long as is necessary for the purpose of dealing with the specific incident or investigation (including any related legal process or proceeding), but shall not use them for any other purpose.
>
> 4. When the Employer intends to use recordings made by the video surveillance system in any legal process or proceeding which specifically relates to the Union or to a member of the bargaining unit, the Employer shall provide the Union with a copy of the recordings prior to their use in the legal process or proceeding.
>
> 5. When the Employer intends to rely on recordings made by the video surveillance system in support of employee discipline, the Union and the employee concerned shall have the same right to access and view the recordings as if they were documents in the central personnel file as provided for in article 4.03(a) of the Collective Agreement.
>
> 6. The Employer shall disconnect and remove cameras 34, 35, 36, 38 and 47 (as identified in the July 4, 2008, award) forthwith.
>
> 7. The Employer shall not change the configuration or use of the video surveillance system or the use of the surveillance product or make any change to this protocol except by first providing the Union with advance notice and the opportunity for discussion in accordance with Article 3.03 of the Collective Agreement. For greater certainty, any such change may be the subject of a grievance as provided for in that article.

7. Other Surveillance - GPS

The BC Privacy Commissioner has issued a series of decisions over the past several years which set out rules for the use of GPS information from cell phones in an employment setting. The rulings have not found much favor amongst employees or amongst unions, but they have clarified the applicable principles.

In *Kone Inc.*[22], the employees complained that the company was not permitted to use the GPS information collected from cell phones under the provisions of PIPA. The Privacy

[22] *Kone Inc.*, [2013] BCIPCD No. 23

Commissioner found that the company could collect and use the GPS information under sections 13 and 16 of *PIPA*, which provide that an organization may only collect or use employee personal information without consent where it is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual". The Commissioner found that the GPS information was "employee personal information" and that the company was collecting and using the personal information for purposes reasonably required under these sections.

However, sections 13 and 16 also provide that an organization must notify an individual that it will be collecting or using that individual's employee personal information and notify him of the purposes for the collection or use before collecting or using the employee personal information. The Commissioner determined that the general privacy policy provided by the company was insufficient to provide the notice required by the legislation. In the Commissioner's opinion, the legislation requires "some degree of specificity" and "meaningful notice" so employees know what types of personal information are being collected etc. (paragraph 80).

In the companion case, *Schindler Elevator Corp.*[23], the Privacy Commissioner completed a comprehensive analysis of the law in relation to GPS technology, introducing her decision with the following statements:

> "This case involves increasingly common and important questions about how technologies that enable business to monitor work related activities to a much greater extent than before affect the privacy of individuals during the considerable portion of their lives spent in the workplace."

In this case, the company used a GPS and engine monitoring technologies on the vehicles used by field mechanics who visit worksites where they repair and maintain elevators. The mechanics worked from home - they kept their vehicles at home and traveled to and from work from there without reporting to the company's office as part of their daily routine. In finding that the company was in compliance with the legislation, the Commissioner addressed a number of considerations, including:

- whether the company was authorized to collect the employee personal information;
- the sensitivity and amount of information;
- whether the collection use or disclosure in question is likely to be effective in fulfilling the company's objectives;
- whether there are other alternatives;
- whether the collection is covert; and
- whether there is an offense to the employee's dignity.

8. Alcohol and Drug Testing

One of the leading Canadian cases on this issue is *Rio Tinto Alcan v CAW-Canada Local 2301*[24]. Rio Tinto claimed to have significant issues with employees missing work due to drug and alcohol use. The policy grieved by the union required employees to submit to medical evaluations. There were significant consequences for employees who refused to undergo the

[23] *Schindler Elevator Corp.*, [2012] BCIPCD No. 25
[24] *Rio Tinto Alcan v CAW-Canada Local 2301*, [2011] BCCAAA No. 17, 204 LAC (4th) 265

medical evaluations, including discipline and possible discharge. The arbitrator found that the creation of mandatory evaluations under the policy violated the privacy rights of employees.

Arbitrator Steeves (now Steeves J.), sets out what has come to be described as “Canadian model” of drug and alcohol testing:

> **37** There are some important differences between an employee's obligation to undergo testing for drugs and alcohol, in particular the consequences for refusing to be tested, compared to situations where medical assessments or opinions are requested by employers in cases where there is no issue of alcohol or drug use. I set out the principles of the so-called "Canadian Model" of drug and alcohol testing as follows (much of the following is taken from *Imperial Oil, supra,* see in particular paragraph 100),
>
> (a) No employee can be subjected to random, unannounced alcohol or drug testing, save as part of an agreed rehabilitative program. This is the case with all employees, including those working in safety sensitive positions (*Imperial Oil, supra,* paragraph 101), although those positions obviously require particular vigilance by Employers.
>
> (b) However, an employer may require alcohol or drug testing of an individual where the facts give the employer reasonable cause to do so. This is a balancing of interests approach and it departs from the proposition in *Monarch Foods, supra,* that an employer could not at common law assert any right to search an employee or subject an employee to a physical examination without the consent of the employee (*Canadian National Railway Co., supra,* at paragraphs 182-189; citing *Trimac Transportation Services - Bulk Systems v. Transportation Communication Union*, [1999] C.L.A.D. No. 750 (Burkett)). ….
>
> (c) It is within the prerogative of management's rights under a collective agreement to require alcohol or drug testing following a significant incident, accident or near miss, where it may be important to identify the root cause of what occurred (and where there is no applicable provision in the collective agreement that addresses the issue). This follows from an employer's responsibility to ensure the work place is safe for the employee who may be tested, for the safety of other employees, for the protection of the employer's property and in some circumstances for the protection of the public.
>
> (d) Drug and alcohol testing is a legitimate part of continuing contracts of employment for individuals found to have a problem with alcohol or drug use. As part of an employee's program of rehabilitation, such agreements or policies may properly involve random, unannounced alcohol or drug testing for a limited period of time, most commonly two years. This is the only exception where the otherwise protected employee interest in privacy and dignity of the person must yield to the interests of safety and rehabilitation, to allow for random and unannounced alcohol or drug testing.
>
> (e) In a unionized workplace the union must be involved in the agreement which establishes the terms of a recovering employee's ongoing employment, including random, unannounced testing.

(f) An employee's refusal or failure to undergo an alcohol or drug test in the three circumstances described above (a significant incident, accident or near miss) may properly be viewed as a serious violation of the employer's drug and alcohol policy, and may itself be grounds for serious discipline. This is a clear difference from the situation with general medical conditions (not involving drugs or alcohol) where an employee may be suspended, and perhaps ultimately dismissed on a non-culpable basis, for refusing to provide the employer with medical information.

(g) The situation with alcohol and drug testing vis-à-vis medical examinations generally can be summed up as follows,

> *... the right that an employer may have to demand that its employees be subjected to a drug test is a singular and limited exception to the right of freedom from physical intrusion to which employees are generally entitled by law. As such, it must be used judiciously, and only with demonstrable justification, based on reasonable and probable grounds.*
>
> *United Transportation Union v. Canadian National Railway Co. (Keeping Grievance),* [1989] C.L.A.D. No. 4 (M. Picher), at paragraph 23; cited in *Canadian National Railway*, *supra*, at paragraph 188

Communications, Energy and Paperworkers' Union Local 707 v Suncore Energy Inc.[25] is an important illustration of the failure of a blanket policy. In this case, the union grieved the employer's policy, stating it was unreasonable because it called for drug and alcohol testing following any accident no matter how minor.

More importantly, the supervisor did not have to believe that drugs or alcohol played a role in the incident. Supervisors were required to test unless they could "rule out" drugs or alcohol. Testing in this manner was found to be an invasion of privacy. The onus should not have been on supervisors to find evidence not to test, but rather to have justification for ordering the test.

The Supreme Court of Canada recently had the opportunity to clarify aspects of the law on this very contentious but important issue in a case originating in New Brunswick: *Communications, Energy and Paperworkers Union of Canada, Local 30 v Irving Pulp & Paper, Ltd.*[26]

The grievor, a millwright in a safety sensitive position, was selected for a random breathalyzer test. The consumption of alcohol was against his religious faith and not surprisingly he felt humiliated and degraded at having to take the test.

The issue of random mandatory alcohol testing made its way to the Supreme Court of Canada which determined that although the workplace was dangerous, what is additionally required in

---

[25] *Communications, Energy and Paperworkers' Union Local 707 v Suncore Energy Inc.*, [2008] AGAA No. 55, 178 LAC (4th) 223

[26] *Communications, Energy and Paperworkers Union of Canada, Local 30 v Irving Pulp & Paper, Ltd.*, [2013] SCJ No. 34; 2013 SCC 34

the assessment is evidence of enhanced safety risks, such as evidence of a general problem with substance abuse in the workplace. The Supreme Court of Canada agreed with the original arbitration board that found the random testing to be unreasonable. The Court summarized its views in very strong clear language as follows:

> A unilaterally imposed policy of mandatory random testing for employees in a dangerous workplace has been overwhelmingly rejected by arbitrators as an unjustified affront to the dignity and privacy of employees unless there is evidence of enhanced safety risks, such as evidence of a general problem with substance abuse in the workplace. The dangerousness of a workplace is clearly relevant, but this does not shut down the inquiry, it begins the proportionality exercise. It has never been found to be an automatic justification for the unilateral imposition of unfettered random testing with disciplinary consequences.
>
> In this case, the expected safety gains to the employer were found by the board to range from uncertain to minimal, while the impact on employee privacy was severe. The board concluded that 8 alcohol-related incidents at the Irving mill over a 15-year period did not reflect the requisite problem with workplace alcohol use. Consequently, the employer had not demonstrated the requisite safety concerns that would justify universal random testing. As a result, the employer exceeded the scope of its rights under the collective agreement.
>
> The applicable standard for reviewing the decision of the labour arbitrator is reasonableness. The board's decision must be approached as an organic whole, not as a line-by-line treasure hunt for error. In this case, based on the findings of fact and the relevant jurisprudence, the decision was a reasonable one.

A somewhat related issue was dealt with in *Canadian National Railway Co. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 100*[27], where the matter of the rights of management, as opposed to the privacy rights of an employee after a conviction for impaired driving, were explored.

Under challenge in this case was the employer's policy whereby employees who drive as part of their employment and lose their driving privileges must report the loss of their license to their supervisor and thereafter be subject to a medical assessment to determine whether they must follow an addiction rehabilitation program. The union argued that the company's policy is an unwarranted intrusion into personal and private information for what the union characterizes as health related issues, highway traffic matters or questions of public policy, and not workplace safety related issues. The arbitration panel disagreed. Persuasive was Dr. Baker's testimony that the chances of an individual charged with a single DUI offense having a substance use disorder are in the range of 40%. In Dr. Baker's opinion, an impaired driving conviction is itself a major flag in respect of the possibility of a substance use disorder - which translates into a risk of danger within a safety sensitive workplace.

[27] *Canadian National Railway Co. v National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 100,* [2013] CLAD No. 249

9. Terrorism - Bio-Security

The interrelated issues of the security of our food supply, management's rights and obligations with respect to that issue, and the right to privacy of individual employees where explored in *Teamsters Local Union 647 v William Neilson Dairy*[28].

As a result of heightened security concerns following 9/11, the employer had taken additional measures to protect the security of the plant which produced fluid milk and other refrigerated products as well as non-refrigerated products. The employer installed an additional 32 cameras (previously there were only 10 cameras) as a bio-security measure. The additional cameras were both internal and external and were motion activated.

The union grieved the installation of 21 of the additional cameras. The arbitrator found that much of the internal video surveillance was warranted by the employer's legitimate interest in maintaining bio-security. Modifications to the surveillance system were ordered for the periods of time during which bargaining unit members were working in the plant to minimize the intrusion of their privacy. As well, cameras were ordered to be repositioned and the areas of coverage were modified.

The arbitrator ordered the following limitations to be applied to the video surveillance.

> **23** As part of the aforementioned balancing exercise, it is also hereby ordered that images obtained from the internal camera system only be used as a tool to investigate bio-security threats or incidents, incidents of health and safety violations, and incidents of culpable conduct, with no real-time monitoring of employees for any other purposes, and no use of those images for purposes of monitoring production, lateness, or attendance. It is further ordered that any images recorded from internal cameras not be retained for more than the aforementioned period of thirty to thirty-seven days (after which they are automatically overwritten by new images), except for the purpose of downloading (to DVDs) images pertaining to bio-security threats or incidents, incidents of health and safety violations, and incidents of culpable conduct. The downloaded images are only to be retained for as long as they are reasonably required for investigative purposes, regulatory purposes, or for purposes of legal proceedings

10. Terrorism - Spousal Background Checks

Perhaps the most intrusive of any legislation that I am aware of in the postwar year is the *Marine Transportation Security Regulations* SOR/2004-144, which came into effect on July 1, 2004 in response to the 9/11 attacks 3 years previously. The regulations contained an elaborate scheme for screening workers in security sensitive positions and the ports of Canada.

It requires employees to provide information about themselves and their spouses in order to determine whether they represented a threat from terrorism or organized crime. The required information included employment, educational, and travel information, as well as spousal

---

[28] *Teamsters Local Union 647 v William Neilson Dairy (Surveillance Camera Grievance)*, [2009] OLAA No. 128; 182 LAC (4th) 403

identity information, to be followed by checks and verification including a criminal record check and if necessary, a CSIS security assessment.

At issue in this particular case was whether the regulations breached *Charter* rights by constituting an unreasonable intrusion into privacy.

The unions argued that those members employed at the Vancouver Fraser Ports comprised a stable workforce. Some of these employees have expressed serious concern that, after many years of employment, they are now regarded as potential security risks, and were subject to extensive background checks which intrude on their privacy and, if the information is shared with foreign governments that have poor human rights records, may also expose them to grave personal danger.

As well, of Canada's many trading partners, only the United States and Australia had comparable background checking systems for port employees. These checks were not required by the International Labour Organization nor the International Maritime Organization, which are responsible for setting international labour and maritime standards, or by the International Ship and Port Security Code.

ILWU also pointed out that, as in other countries, ports in Canada already have physical security measures in place, such as fencing, lighting, patrols, and x-ray and radiation screening. However, the Attorney General notes that it is always possible for an "insider" to subvert these measures.

The court referred to the Supreme Court of Canada decision in *R. v. Beare*[29] in noting that photographs and fingerprints were the least intrusive forms of search. On the issue of the complete absence of any indication of prior terrorist activity, and on the issue of the extraordinary demand for the subjecting of an employee's spouse to these security measures the court had this to say:

> **64** The fact that employees have not been the source of terrorist activities in the past is no guarantee that some may not be in the future. In this context, it is important to recall that the Regulations are also intended to protect against threats from organized crime which, for a price, may offer its services to terrorists by aiding them in, for example, smuggling weapons, explosives or operatives into Canada in containers.
>
> **65** In my view, the evidence taken as a whole establishes that the Government is right to take seriously the possibility that port security could be endangered from the inside by employees acting from ideological or mercenary motives. Nor is it implausible, as Professor Wark agreed, that an employee could be influenced by a spouse or partner, present or past, to engage in such activities.
>
> **66** The fact that Canada may have the world's most rigorous system for conducting background checks on port employees does not in itself render it unreasonable. Canada's long coast line and many ports, its substantial economic dependence on international trade in goods transported by sea in and out of Canada and, to a lesser degree, on cruise line business, its ability to fund security measures, and its proximity to

[29] *R. v. Beare*, [1988] 2 SCR 387 at 413

> the United States, are all factors that provide a rational explanation of why Canada has instituted the present security clearance system.
>
> **67** These considerations also indicate the substantial and pressing nature of the public interest that the Regulations are designed to advance: protection from threats to public safety and the economy from the activities of terrorist groups and organized crime.
>
> **68** It is, of course, always possible that errors will occur and that an employee may become the object of suspicion on the basis of erroneous information used for background screening. For example, doubts have been expressed by the Auditor General about the reliability of information held by the RCMP in exempt data banks. However, an employee has an opportunity to correct an error in representations made to the Minister after being advised of the basis on which the Minister is considering refusing a security clearance. It would be open to an employee to apply for judicial review of a refusal of a security clearance for breach of the duty of fairness on the ground, for instance, of inadequate disclosure of the basis of the refusal.
>
> **69** I am not persuaded that, in view of the potentially grave nature of the threats to the security of maritime transportation from terrorists and organized crime, the information required by the Regulations can be said to be overly intrusive and insufficiently tailored to the perceived risks. Accordingly, the search authorized by the Regulations is not unreasonable and does not violate section 8.

11. Biometrics: Management Convenience vs Privacy?

At its simplest, biometrics involves the use of part of the body as a unique identifying feature of each individual employee.

One of the leading Canadian cases assessing the use of biometrics in the workplace is *Agropur, Division Natrel v Teamsters, Local 647*[30]. The company planned to introduce a time management system that included mandatory fingertip scans of employees. The system would replace the classic punch card system with the swipe of an individual access card, and a verification of identity with a finger scan. An employee clocking in or out would place a finger on the biometric reader and his or her identity would be verified if the fingertip scan matched the one stored in the system. The arbitrator stated:

> **35** ….[T]he issue in this case is whether this employer's plan to institute a biometric element in a new timekeeping system intrudes on those privacy rights in a way that is unreasonable. Both parties in this case, while arguing for different results, urged the same method of analysis: the reasonableness of the employer's requirement that employees must submit a fingertip scan must be judged by balancing the employee's interest in privacy against the employer's reasons for requiring an infringement of that privacy. To that I would add that I agree with the view as expressed in the *Canada Safeway* case and others that proportionality is a key tool in assessing whether the infringement of privacy is justified: the more intrusive the impact on employee privacy, the greater the business rationale that must be demonstrated.

[30] *Agropur, Division Natrel v Teamsters, Local 647* [2008] OLAA No. 694

The one benefit the finger scan provided over the introduction of a new electronic system which would achieve most of the employer's objectives was that it would eradicate any practice of one employee punching another employee's card for him or her at the start or close of the shift, what is sometimes awkwardly described as 'buddy punching'. The only evidence of that practice was that there had been a small number of incidents over the past 2 years. Everyone acknowledges there was no evidence of it being a rampant practice. Although they also acknowledged that if it was the substantial practice in the workplace it may well not be detected.

To pause here for a moment in our review of the case, the above proposition identifies one of the concerns expressed about some of the case law in this area – that the justification for the incursion into employees' privacy rights is based on speculation as to the existence of the workplace problem, or as here, the magnitude of the workplace problem. The *Agropur* arbitrator characterized the business rationale as legitimate although not a pressing or crucial one.

Turning then to an assessment of the infringement on employee privacy, the arbitrator characterized it as extremely small, almost negligible. In fact, the arbitrator offered the opinion that characterizing a finger scan as an invasion of privacy struck him as a 'linguistic excess'. It involved less than half of the fingertip and took less than a minute. He pointed out there was no physical intrusion, no furnishing of any bodily substance, no exposure of any private part of the body.

The scan was immediately converted into a template based on a mathematical representation and the scan itself is deleted. That template is retained for verification of identity when the employee clocks in. It is in a form virtually useless to anyone on its own. There was no personal information provided about the employee. The scan was not a fingerprint and could not be reconstructed into a fingerprint. The resolution of the scan is far lower than that used by law enforcement agencies. Finally, the templates were stored in a secure computer server, and are deleted when employment is terminated.

Of interest is the fact that although the arbitrator determined that the employer's business rationale was not pressing or crucial, he found that it was "too much to ask an arbitrator to stop an otherwise justifiable exercise of management rights based on speculation of future abuse".

12. Biometrics - Function Creep

The issue of facial recognition technology (FRT) has yet to surface as a major issue in the employment context, but is likely too soon. I include this following case for the Privacy Commissioner's discussion of facial recognition technology in the context of privacy. Like all technology of this kind that ultimately affects a right to privacy, it also has a legitimate utility – in this case to protect against identity theft. It can be used to quickly and accurately compare millions of images to determine whether an individual is the person he or she claims.

In addition, no one quarrels with the proposition that identity theft is becoming increasingly common, some estimates suggesting as many as 2000 complaints of identity theft in this country every month. It is a factor in bank, credit card, and document frauds.

But then, to quote from the decision of the Privacy Commissioner in *British Columbia (Insurance Corp.)*[31]:

> **35** "Biometrics" is literally, the measurement of life. It refers to the technology of measuring, analyzing and processing the digital representations of unique biological data and behavioral traits such as fingerprints, eye retinas, irises, voice and facial patterns, gaits, body odours and hand geometry.[13]
>
> **39** …. FR technology has also been described as "one of the gravest privacy threats of our time."[18] Privacy experts, particularly in Europe and North America, have identified a number of significant privacy concerns associated with FR technology.[19] The two most significant ethical and privacy implications of biometrics are function creep and the use of our bodies as identification tools.

This particular investigation arose in the aftermath of the Vancouver Canucks Stanley Cup loss in June 2011, where ICBC volunteered the use of its facial recognition software to assist police in identifying alleged vandals and rioters, from the hours of video tape and still photography before, during and after the riots. The Vancouver Police Department did not act on the offer, either out of its own good judgment, or as a result of the storm of public protest that developed once ICBC's peculiar brand of volunteerism with others privacy rights became publicly known.

The issue of function creep is of central importance in understanding the significance of technology in the context of any concern for privacy rights. This case provides a classic illustration of the difficulties those charged with protecting our privacy rights face in highly politicized circumstances such as the Stanley Cup riots. The event was a huge civic embarrassment, with all levels of politicians including the Premier weighing in on the discussion, and promising speedy apprehension and trial of those responsible.

> **40** Facial recognition is now available on social networking sites, has been implemented on video surveillance cameras and used at large public events to identify attendees.[20] With the implementation of facial recognition individuals will no longer be able to remain anonymous in public places. The system may, in a matter of seconds to minutes, identify you to the public body or organization running the facial recognition software. Previously private political, religious and social affiliations will now become public.
>
> **41** Use of our bodies as identification tools--FR technology has the potential to change our relationship with the world. Deciding what information about ourselves we will share with others helps define the boundaries of different relationships. One shares more of himself with a friend than with an employer, more with a life-long friend than with a casual acquaintance. The ability to keep parts of our lives private is central to our ability to feel unique-when our lives are laid bare for all the world to see, we can take no more ownership over them than anyone else.[21]
>
> **44** Function creep-Function creep occurs when a process or system intended for one purpose is subsequently used for a new or originally unintended purpose. When personal information is involved, function creep implies that the change in use is without the knowledge or consent of the individuals.

---

[31] *British Columbia (Insurance Corp.)*, 2012 BCIPCD No. 5

> **45** Function creep is a particular concern in biometrics because biometrics is a very powerful identification tool and because databases are becoming increasingly interoperable.
>
> **47** Function creep is a privacy issue because it is a basic privacy principle that personal information should only be used for the purpose it was originally collected unless, in the case of public bodies, FIPPA permits a change in use. Such a change in use should be subject to careful scrutiny given the sensitivity of biometric data and its potential for interoperability with other systems.
>
> **62** Section 27 of FIPPA requires that where a public body collects personal information directly from an individual--such as when ICBC takes photographs of citizens--the public body must ensure that the individual is told the purpose and legal authority for the collection. The notice must also include contact information for an employee within the public body who can answer questions.
>
> **63** Notification allows the public to understand the purpose, nature and extent of collection of personal information. Without proper notification, the public is unable to ensure that their rights under FIPPA are preserved. Individuals unaware of the use of biometrics such as facial recognition, cannot object to or question the technology.
>
> **64** ICBC advised that the purpose for the implementation of FR technology in November 2008 was to enhance the security of BCDLs and BCIDs by detecting and preventing fraudulent use or obtaining of these documents.
>
> **65** ICBC provides some notification in the following two ways: (1) on the Driver Statement of Declaration provided with interim licenses and (2) on signage in some, but not all of its offices. The notices make no reference to the use of FR technology, nor to the use of the information for the purposes of preventing fraudulent use or obtaining of drivers' licences or BCIDs.

The Commissioners conclusions were as follows:

- That the use of ICBC's FR database to assist police was a change in use**.** (This is essentially function creep, which is the major concern of collection/use of biometrics.)

- This change in use would require a subpoena, warrant or order to be compliant with FIPPA, otherwise, the use of ICBC's FR software and database for the purposes of responding to disclosure requests for police was not authorized under FIPPA.

The report also mentions that prior to the riot, since January 2011, the police had made 15 requests to ICBC to use its FR database in other identity cases. In at least one of those cases, ICBC had provided information with respect to the possible identity of the individual. During the Privacy Commissioner's investigation, ICBC ceased accepting or responding to police requests pending the results of the investigation.

Conclusion

My assessment of the current state of employee privacy rights in the context of arbitral jurisprudence and Privacy Commissioner decisions is simple. Unions have been remarkably

successful in pressing their concerns on behalf of their members over the preservation of workplace privacy rights. The protocol for example, that was set out in the *Cargill* decision for video surveillance cases, and the principles adopted by the arbitrator in *Rio Tinto* provide a remarkable degree of protection, while at the same time recognizing the legitimacy of the employers interests at stake.

The one exception to that generalisation is in the area of biometrics. Two cases illustrate the reasons for my concern. In the *Agropur* case [page 16 above], the arbitrator was dismissive of the union's concern about possible future use of fingerprint scans, suggesting that was too speculative as it was based on technology that did not yet exist. He characterized the union's description of finger scans as 'an invasion of privacy' as almost a linguistic excess. Yet he was prepared to approve finger scanning in the workplace on the basis of the scantiest evidence of any real workplace problem - only a small number of cases of employees completing time cards for other employees – buddy punching - over a two-year period.

The second case is not an employment case, but has implications for employees. It is the decision of the BC Privacy Commissioner in *British Columbia (Insurance Corp.)* [pages 17/18 above]. My concern does not arise from the Commissioner's decision itself, which I largely agree with. Rather my concern arises from the conduct of ICBC, one of the largest public corporations in the country, and a unionized employer, that was revealed in the case. The decision disclosed that ICBC had readily volunteered drivers' license personal information - facial photographs - to aid a police investigation. As ICBC is a monopoly, at issue were the privacy rights of virtually the entire adult driving population in the province. ICBC volunteered this personal information without soliciting the consent of the individuals involved, and indeed without formally notifying the individuals as to what it was doing. Its complete lack of appreciation of the importance of privacy rights is difficult to grasp.

Turning from the employment context to the broader public context, the developments in the past several years as a result of the Snowden disclosures are extremely worrisome. We now know, along with the citizens of the US and Britain, as well as Canada, that the major violator of our privacy rights are the very government(s) whom we trusted to protect those rights.

For example, according to the *Globe and Mail*, Defence Minister Peter MacKay signed a ministerial directive in November, 2011, authorizing the re-start of a secret electronic eavesdropping program that scours global telephone records and Internet data trails – including those of Canadians – for patterns of suspicious activity. All of this was done of course without any notice, and as important, without any persuasive evidence that it would be productive, or that other less intrusive methods would not be effective.[32]

[32] Daniel Tencer, *Canada Has NSA-Style Surveillance System, Documents Show* (06 October 2013), online: The Huffington Post <http://www.huffingtonpost.ca/2013/06/10/nsa-surveillance-canada-_n_3416730.html>