Alberta Federation of Labour

WORKPLACE PRIVACY

INTRODUCTION

There is no doubt Albertans would feel uncomfortable if some stranger was accessing their medical records, tracking what websites they visit or recording what they say on our phone calls. But how would they feel if that stranger was their boss?

Most people know they have a right to privacy in their personal lives and the reasonable limits to that privacy. However, few workers know what rights they have at work to protect their privacy. Do workers have privacy rights at work? What is the boss allowed to see? And what are they do to about the battery of new technologies at employers' disposal to monitor their activities, health and behaviour?

Invasions of privacy can take many forms in the workplace. It can involve monitoring of activities, collection of personal data, invasive questions, tracking geographic location, inappropriate use of personal information, or giving out personal information.

There is a pressing need for the labour movement to establish a position on the issue of workplace privacy. We need to establish a clear set of principles upon which we can challenge employer attempts to restrict our privacy at work.

OLD TRICKS, NEW TOOLS

Since the Industrial Revolution, employers have demanded the right to access personal information about their workers and to monitor activities at the workplace. The picture is not new: managers hovering over workers to scrutinize their every move; supervisors measuring, stopwatches in hand, productivity levels; company doctors poking and prodding to determine fitness to work; private detectives hired to see if an injured worker is "really" injured. These methods are as old as management itself.

Today a new set of tools has been added to these old tricks. Electronic monitoring and surveillance, Global Position Systems (GPS), health testing, biometrics and other innovations give employers an unprecedented capacity to invade and capture, increasing the level of concern workers should have about employer monitoring.

Whether it is the old-fashioned stopwatch or the new-fangled GPS, one constant is the employer's motivation for gathering worker information. Employers have always been

driven to gather information about workers, and they do so for three reasons. First, it is about ensuring an acceptable level of productivity or quality of job performance. Observation and data collection is most often driven by a need to make sure workers are doing their job the way management wants them. In short, collecting worker information is just another management technique for maximizing productivity, quality and profit.

Second, employers may monitor for the purposes of safety and/or security. Often it is to protect property from damage or theft – either from workers or the public. Sometimes it can be about worker safety – preventing accidents or ensuring an appropriate disability accommodation.

Third, it can sometimes be nothing more complicated than control. Watching over a worker, asking personal questions about medical history, listening in on telephone calls, requiring drug testing and so on send a clear message to workers who has the most authority and power at work. By demanding information, employers can take advantage of both the employment relationship and the workers' vulnerability in that relationship (fear of dismissal, reprisal) to obtain information AND increase workers' feelings of insecurity. By doing so, they hope to achieve a more compliant workforce.

Control can even apply to HOW an employer uses personal information. Letting out sensitive medical or financial information about a worker can damage that worker's reputation, capacity to work or personal life. Such abuse of privilege is often about control and power – exercising the ability to harm another person due to their position.

While the motivations are ages old, the new technologies and techniques create a new kind of threat. New methods allow for a deeper intrusion into workers' lives. Employers can now easily gather biological and genetic information, delve into recreational activities through drug testing and overhear private conversations through electronic monitoring. "Today, new technologies present employers with an ability to monitor employees at an unprecedented level. Not only do new technologies exist for the act of monitoring, … but new technologies also exist for the processing of information gathered by monitoring. Employers now have the capability of processing and retaining vast amounts of information." (Levin *et al.*, 2006; 1)

Employers have an expanding catalogue of techniques and methods at their disposal to monitor workers and collect information about them. Here are the ways employers invade the privacy of their workers:

1. ***Electronic Surveillance***: The use of video or audio collection to monitor workers and/or public areas. It can include closed-circuit TV or taping of telephone communication. Workers are under constant surveillance in these systems, their every move recorded.
2. ***Access Control***: The use of ID cards, swipe cards or other techniques to restrict access to certain areas. While mainly about security, these systems also allow

employers to track when workers come and go from the area and allow them to follow worker movements and location.

3. ***Digital recording***: The tracking of worker computer activity by keeping email records, maintaining web traffic logs or recording keystroke patterns. Every electronic action the worker takes can be monitored, recorded and compiled.
4. ***Biometrics***: The collection and use of personal biological properties (e.g., fingerprints, retina scans, voice recognition) for access control or other security features. Worker movement can be recorded, but fundamental biological information is captured and stored by the employer, posing security risks to the worker if the information is misused.
5. ***Global Positioning/Radio Frequency ID***: Satellite tracking (GPS), or radio frequency tags (e.g., retail tags attached to clothes to prevent theft) can be installed on virtually any vehicle, product or person to allow the employer to know at any time where the tagged item is. This allows for precise, real-time, 24-hour tracing of worker or product location.
6. ***Health Information Gathering***: The collection of medical information (e.g., urine or blood samples, responses to psychological tests, doctor's reports) for use in investigations, security, hiring, disability accommodation or other uses. Other forms of medical information gathering include company doctors, nurses and occupational health and safety departments as well as Employee Assistance Programs (EAPs).

The six main methods for collecting information is only the first potential area for privacy abuse by employers. Once employers have information, how they use it and to whom they disclose it also pose risks. An employer may use the information for disciplinary purposes, or to justify altering the labour process. Or the employer may release the information to a third party, or a supervisor. All of these actions have the potential to harm the privacy rights of workers.

THE COST TO WORKERS

Employers consider their intrusions justified and even necessary. In many cases that may be true (such as gathering health information to accommodate a disabled worker). But even if legally allowed, the employer prying into the personal information of workers still exacts a cost.

Take a relatively mundane task of collecting payroll information – address, family status, SIN, etc. While it is perfectly acceptable for the employer to collect this information, it still makes the worker vulnerable. What if the information is stolen or misused? It is the worker who would experience the negative consequences of something going wrong, not the employer.

Workers are affected in three clear ways when an employer, appropriately or wrongly, gathers and uses personal information on the worker. First, the worker's rights to privacy are violated or have the potential to be violated. Personal information is sensitive because its use has real consequences. Medical information, home address, SIN, age, sex, etc., all have repercussions for workers if misused. Identity theft is a real worry.

Rumours and innuendos can develop and spread from personal information. Financial, personal and professional relationships can be damaged. Plus, the gathering may breach one of the laws governing privacy.

Second, employer gathering of personal information increases worker vulnerability and insecurity as mentioned previously. When an employer gathers information about its workers, that information can be used to evaluate, discipline or dismiss. Workers have legitimate cause to feel more insecure when employers gather their information. How will the information be used? It can also lead a worker to feel not trusted by his/her employer or feel his/her ability to perform the job is being questioned. "Studies have shown that in workplaces where there is an excessive degree of monitoring, there is a correspondingly high degree of employee stress." (O'Donoghue, 2001; 4)

Third, invasion of privacy, even justified, results in the loss of personal integrity for the individual. As Jennifer Stoddart, Privacy Commissioner of Canada wrote, "Workplace privacy is an important part of the basic autonomy rights of individuals in our society." (Stoddart, 2006) When someone gathers our information, a piece of the protective shield around our identity and our sense of self is breached. We often allow this breach for the benefits of doing so may be clear. But even when we allow it, we experience vulnerability for doing so. We know such information can potentially be misused and it undermines our sense of personal integrity.

DO WORKERS HAVE PRIVACY RIGHTS AT WORK?

So, what does the law say about workers' privacy rights at work? Do they have any? Or is it an unfettered field for employers to do as they wish?

The answer is not simple. In the U.S., they adopt what is called the "property approach" which suggests that because the employer owns the workplace and the activities within it, workers have no inherent privacy rights. "As a result of this ownership, employers are free to dictate to employees ... and employees only have privacy rights, or more accurately expectations of privacy, to the extent that employer policies allow." (Levin *et al*., 2006; 1)

Meanwhile in Europe, a "rights approach" has been adopted. It is based upon "a belief in the dignity and right to private life that is afforded to every human being. ... Employees are entitled therefore to some minimal standard of dignity, privacy and a private life even while working and while using workplace resources". (Levin *et al*., 2006; 1)

In Canada, law makers and arbitrators have attempted to craft a compromise between these two approaches. "Privacy is not an absolute right, and in the workplace, is balanced against the employer's legitimate need to maintain a safe, efficient and productive workplace." (O'Donoghue, 2001; 1) Canada's attempt at a "balance approach" has led to two outcomes. First, workplace privacy issues are more complex in Canada and often rest upon the specific facts of individual cases. Second, the shifting ground that results creates more confusion and uncertainty for both employers and workers.

The fundamental flaw in the Canadian approach is that it assumes the two interests can be easily and successfully reconciled – that worker and employer can find common ground on privacy. This is often not the case, as a worker's right to privacy and an employer's need for information are often irrevocably at odds, creating difficult, if not insurmountable, challenges to finding a place of fairness.

In addition, the "balance" approach suggests that a person's identity and integrity are on equal footing to an employer's desire for higher productivity and control. This is patently false. One is embedded in the concept of human rights and dignity, while the other is an unavoidable part of the employment relationship. One is a natural right; the other an economic construction. To suggest balancing these two rights is to undermine the validity of privacy rights.

LEGAL STATUS OF EMPLOYER ACTIONS

Much of the confusion about the state of workplace privacy is that there is no one body of law to which to refer. Depending on where you are, which industry you work in, and the nature of the information in question, a different set of rules will apply. The *Freedom of Information and Privacy Act* (FOIP) relates to Alberta public sector, while the *Personal Information Protection Act* (PIPA) addresses the private sector. Unless the information is health information, in case it is the *Health Information Act* (HIA). If you are federally regulated, you are covered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Then there are the *Human Rights, Citizenship and Multiculturalism Act* (HRCM) and the *Charter of Rights and Freedoms* for human rights issues.

For occupations with regulatory professional bodies (registered nurses, social workers, etc.), the legal situation becomes more complicated, as issues related to the governing legislation and the body's standards and disciplinary panels insert themselves. These bodies can require or encourage additional breaches of worker privacy. They can also enhance privacy protection.

Interpretation of the law is equally segmented, with the courts, arbitrators, human rights commissions and privacy commissioners all weighing in on privacy. In sum, it is all very confusing and at times contradictory.

It is a difficult area of law to summarize, but some basic principles have been established:

- Consent is paramount. If consent is given, the employer is free to collect, use, or disclose the information. (Unless the consent was not given freely or compromises a fundamental human right.) Collection/use without consent is permitted, but in much more narrow circumstances.
- The employer collection/use of information must be specifically and only related to the employment relationship. (OPCC, 2004)

- The collection/use must be deemed as "reasonable" under the circumstances. This is determined with a four-part test (as laid out by the Federal Court of Canada in Eastmond v. CP Railway, 2004):
    1. *Is the measure necessary to meet a specific need?*
    2. *Is it 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?*
- Personal information must be treated confidentially, used only for the expressed purposes for which it is gathered and not released without the knowledge of the person involved.
- Reasonable notice of the collection/use must be given to workers.

Of course, if a union collective agreement explicitly prohibits a particular form of information gathering or monitoring, then the contract provisions will prevail. An agreement may also allow information collection/use as long as it does not contravene human rights.

In interpreting "reasonable," some patterns have emerged in commissioner, arbitrator and court decisions. Some include:

- Surveillance is permitted for legitimate security (e.g., theft prevention) or safety (e.g., ensure worker safety) purposes, but the data collected cannot be used for any other purpose.
- Surveillance is permitted for investigative purposes (e.g., accident investigations), but such collection must be specific and not applied to all workers or all times.
- Workers must be informed of any monitoring or surveillance in the workplace and the purposes for which it is being collected/used. There are very few exceptions to this.
- Monitoring for productivity/work quality purposes (e.g., recording calls, video, keystroke recorders) is only permitted in a narrow range of circumstances. Generally it is seen as "unreasonable."
- Employer access to health information is much more limited. It must be "only information that is relevant to the employee's job duties." (Alberta Human Rights Commission, 2009; 5) Past medical history, diagnosis, treatment and communicating with health professionals directly are forbidden.
- Testing (e.g., drug, psychological) is only allowed in a limited range of circumstances.
- Company-paid health professionals are permitted and are allowed to collect health information within the scope of their profession. However, they are only allowed to share limited information to the employer – information that relates only to job duties. Other information (diagnosis, past history, etc.) must remain confidential. Workers always maintain the right to see a health professional of their choice.

There are few clear-cut answers to a worker's question about the legal appropriateness of an employer intrusion. For example, drug and alcohol testing is allowed for safety

sensitive and post-incident, but random testing of all workers is not allowed. Electronic keystroke monitoring or e-mail recording is allowed, but not for disciplinary purposes. Closed-caption TV is allowed for security, but not for productivity monitoring. The picture is complex.

In short, workers do have privacy rights under Canadian law, but their ability to exercise them is bounded by a myriad of specific circumstances. There are real prohibitions and restrictions on employer monitoring and information collection. What those specific restrictions are, however, depend on the particular situation in the workplace.

An encouraging sign is that the general trend in Canadian law is toward greater protection of worker privacy. "In years past, an employee's reasonable expectation of privacy alone was determinative. No longer. The emergence of Charter values of privacy, national privacy legislation, international privacy norms, and labour case law all point to a shift towards greater privacy protection in the workplace." (Geist, 2002; 38)

UNION PRINCIPLES FOR WORKPLACE PRIVACY

Unions need to become more active in protecting our members' privacy interests. Employers have become more active in pursuing privacy-invading initiatives. Unions have responded by challenging individual actions through arbitrations and court cases but have not mounted a coordinated, generalized response to privacy invasions. For example, in 2004, only 1.4% of collective agreements in Canada contained clauses dealing with electronic surveillance. (Kiss & Mosco, 2005)

To begin building a more comprehensive response to privacy issues, we must begin by establishing some union principles for workplace privacy.

The Alberta Federation of Labour and its affiliates agree to the following principles:

1. Workers own all of their personal information. Even at work, a worker maintains control over his/her information.
2. Worker personal information includes all of: personal data (address, SIN, etc.), biological and health information, verbal communication, information on his/her activities, location and behaviour at any moment in time.
3. Any act by the employer to collect or use a worker's information shall be seen as an intrusion of privacy.
4. It is recognized some collection of worker information, even if it results in an intrusion of privacy, is required and desirable for the maintenance of the employment relationship.
5. Employer intrusion of privacy shall be seen as legitimate only if the intrusion meets the following criteria:
    a. minimizes harm to the worker's dignity; and
    b. one of the following:
        i. benefits the worker;

   ii. is necessary to deliver a right to a worker (e.g., payroll, disability accommodation); or
   iii. will protect workers from potential harm or injury.
6. An intrusion shall be considered an illegitimate invasion of privacy if it:
   a. Is done without the full and free consent of the worker;
   b. Is intended for evaluation or monitoring of work performance;
   c. Is intended for purposes of discipline, punishment or dismissal;
   d. Contravenes the collective agreement; or
   e. Generally fails to respect the dignity of the worker.
7. The employer must obtain the consent of both the union and the worker before intruding upon the privacy of any worker.

STEPS FOR CHALLENGING EMPLOYER INVASIONS OF PRIVACY

To respond to employer attempts to restrict worker privacy, unions need to develop a strategy. We need to be aware of the specific steps we need to take to prevent invasions of members' privacy. The steps unions commit to taking to protect worker privacy include:

1. ***Grievances***: Where possible, grievances should be launched to prevent unwarranted monitoring of worker activity and collection of information.
2. ***Collective Agreements***: Unions should undertake to negotiate privacy protection language into their collective agreements to firm up privacy rights.
3. ***Legal Recourse***: Unions should make full use of the various legal means through which to protect privacy rights, through arbitrations, human rights commissions, privacy commissioners and the courts.
4. ***Education***: One of the most effective methods to protect against employer intrusions is to educate members on how to remain vigilant to invasions of workplace privacy.
5. ***Collective Action***: Unions will always reserve the right to take collective action to defend our members' interests. This can be one area where we can use the strength of our solidarity to protect our individual and collective rights.

Sources:

Alberta Human Rights and Citizenship Commission, "*Obtaining and Responding to Medical Information in the Workplace,*" January 2009.

Geist, Michael, "*Computer and Email Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance,*" University of Ottawa (Faculty of Law), March 2002.

Kiss, Simon & Vincent Mosco, "*Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada*," Canadian Journal of Communications (Vol. 30, 549-564), 2005.

Levin, Avner et al., "*Under the Radar? The Employer Perspective on Workplace Privacy,*" Ryerson University, June 2006.

O'Donoghue, Mary (Senior Legal Counsel, Ontario IPC Commission), "*Reasonableness in the Context of Workplace Privacy*," speech delivered June 25, 2001.

Office of the Privacy Commissioner of Canada, "*Fact Sheet: Privacy in the Workplace.*"

Stoddart, Jennifer (Privacy Commissioner of Canada), "*Finding the Right Workplace Privacy Balance,*" speech delivered November 30, 2006.

JF:lc*cope458 G:\EVENTS\2009 Convention-Edmonton\Policy Papers\FINAL\FINAL - Policy Papers 2009.doc
Adapted at 2009 46th Constitutional Convention