Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

THE EMPLOYMENT RELATIONSHIP AS THE PRIVACY LABORATORY

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Keynote Presentation to the

Privacy, Law and the Contemporary Workplace Conference
Faculty of Law, Queen's University (Toronto)
November 22, 2013

Good morning and thank you for inviting me to this great conference. I'm honoured to kick things off and I'm sure the rest of the program will get you thinking and talking about a number of key decisions in the courts and technological changes affecting the workplace.

Congratulations to the organizers for the design of this conference, and the many experts, in Canada and beyond who will address us today. I am also told that in addition to faculty and practitioners, that over 20 per cent of you are students. I am very pleased to see you here, the future leaders in this field, and hope that you will stand up and ask questions and provide commentary throughout the day.

I want to spend my time today talking to you about new technology, new expectations and social change affecting the workplace. I want to put some of these changes in context. They relate to the exponential growth in uses of personal information across all sectors of society.

Questions of surveillance and privacy are among the most pressing issues we face in our increasingly digital society. These issues are top of mind to Canadians, particularly post Snowden revelations. Ten years ago in our office, we saw very few complaints or inquiries about privacy in the workplace. Today, over 30% of our privacy complaints and calls are about the workplace. We are all grappling with new technologies, shifting social norms, and new risks to both employers and employees in our increasingly connected world.

Laboratory of Privacy Law

As I was preparing for this presentation today, I was thinking about the many ways in which employee privacy is a unique subset of privacy law. And it struck me that employee privacy is like the laboratory of privacy law. Not because I see employees as test subjects whose rights are to be sacrificed for the greater good, but because the different (and perhaps even opposing) interests between employer and employee gives us an extraordinary place to examine the limits of privacy laws and policies. In other words, the employment relationship incubates the most intense conditions for privacy-related conflicts to arise.

What are those conditions?

First, the "free market" provides little pressure on employers to respect employee privacy. Unlike business-consumer relationships, rarely can an employee simply walk away from their employer because they do not like a given privacy practice. Particularly in challenging economic times, most of us do not have the luxury of being able to choose among a wide variety of employment options, and an organization's privacy practices are probably not a significant consideration for the majority of job seekers.

Second, employees and employers are forced to get to know each other in an inherently close relationship. Employers need to know certain details about their employees, if only to be able to add an employee to payroll and deduct taxes. But, as we all know, the relationship often requires much more.

Employee Information Types

An employee may provide banking information to allow for direct deposits. Background checks may be required where an employee is handling secret information or dealing with vulnerable clients. Sensitive medical information is often necessary in order to qualify for health benefits. Biometric information may be needed to use sophisticated access controls.

The list goes on and on. And that only includes information that is "formally" collected. Employees and managers can get to know a lot of sensitive personal information about each other throughout the course of the relationship.

For example, employees often share details about highly personal medical conditions or family-related issues with a manager when explaining why they need time off. Furthermore, personal friendships and relationships often form in the workplace and this always involves the exchange of personal information. And, because the actions of a rogue or careless employee can have a significant impact on an organization, employers often feel the need to check-up on their employees.

Surveillance cameras are often used to prevent theft by customers and employees alike, although the impact on the employee relationship can be much more significant given the apparent lack of trust, and the amount of time under which their daily lives is subject to surveillance. Similarly, employers often feel the need to monitor electronic communications in order to ensure that employees are not stealing company secrets, or compromising data security through careless actions. Employers may seek to conduct drug or alcohol testing on employees in positions where safety is a concern. Or, surveillance may be simply motivated by the desire to improve efficiency and ensure that employees are not wasting time.

For private sector employers in BC, consent is not necessary to collect, use or disclose personal information that is reasonably necessary for the purposes of managing the employment relationship. This is an explicit recognition of the unique nature of the employment relationship; the relationship simply can't function without a certain amount of personal information.

There is an inherent compromise—employees must give up a certain amount of privacy in order to engage in the workforce. However, employers do not have carte blanche and must be able to demonstrate and justify their purposes.

So given these conditions, what are some of the most important privacy issues we are seeing in the privacy laboratory that is the employment relationship? Well, anyone who has read my office's findings with respect to the use of vehicle monitoring systems to track mobile employees won't be surprised if I begin with this issue. Toward the end of last year I issued a decision concerning the use of vehicle monitoring systems by a private sector company: *Schindler Elevator Corporation*, and another decision about the use of similar technologies by the University of British Columbia. These decisions were published in December 2012 and February 2013, respectively (followed by two additional decisions: TKE and Kone in recent months). In both Schindler and UBC, I ultimately found that employers were authorized to use the systems, but only after lengthy and careful consideration.

In both *Schindler* and *UBC*, the systems are similar: they combine GPS technology to track employees' vehicle location with devices that monitor such things as distance, speed, acceleration, deceleration, idling time, and the time of day when the vehicle is turned on and off. Both Schindler and UBC argued that the information collected and used by the systems was about the vehicles, and merely related to the employees who drove them. In other words, they could do whatever they wanted with the systems because it did not involve the use of personal information.

I disagreed. After a careful analysis of legislation and jurisprudence across Canada—which is remarkably consistent on the meaning of personal information—there is little doubt that the data collected and used by the vehicle monitoring systems is, in fact, personal information about the employees who drive those vehicles. To conclude otherwise could have significant implications for the ability to apply privacy legislation to technologies that all of us interact with on a daily basis.

For example, the police might then argue that our browsing history is information about our computer, and not the person using it. Similarly, it might allow advertisers to use location data from GPS-enabled smart phones without notice or consent, on the basis that the information is about the smart phone and not the user.

With respect to Schindler, I ultimately concluded that the information collected and used through its system was "personal employee information"—meaning that it is reasonably required to manage the employment relationship. Schindler demonstrated that it was using the system to manage productivity , map routes, manage hours of work, and ensure that employees drive safely and lawfully - all of which we concluded to be legitimate, reasonable business purposes.

Similarly, we found that UBC's purposes for using vehicle monitoring were reasonably necessary and compliant with the purposes of the *Freedom of Information and Protection of Privacy Act*.

It's important to note that, in both cases, we were satisfied that managers were **not** engaged in continuous, real-time surveillance of employees. Rather, the systems are designed to raise flags if certain behaviour is identified, or to investigate a safety-related incident after the fact. The line between these legitimate uses and continuous, real-time surveillance may seem like a fine one, but it is critically important.

Before moving on to explore other issues in the employment-privacy lab, I should take a moment here to explain how the federal law in Canada works when it comes to employment-related issues.

Personal Information and Protection of Electronic Documents Act (PIPEDA)

While dealing with PIPEDA is no longer something I do on a day-to-day basis, some of you might remember that I was previously the Assistant Commissioner at the federal level. During my time in Ottawa, I learned a lot about employment-privacy issues, like, for example, how the federal law only deals with employment-privacy issues for those organizations that are federal works and undertakings (banks, airlines, telecommunications etc.).

The biggest issue for these organizations is that unlike BC law, the requirement to gain employee consent is a requirement that has been dealt with uniquely by the Federal Court—specifically the Federal Court of Appeal.

The Court had the occasion to examine the consent requirement in the somewhat famous TELUS "voice printing" case. In that matter, TELUS started a program that required employees to use their voice to authenticate themselves prior to accessing certain sensitive areas of their network. Some employees objected to the use of their voiceprint by their employer and the matter was eventually heard by the Court. After concluding that the collection and use of the voiceprint was reasonable in the circumstances, the Court went on to say that…

> …if an employer is acting reasonably in the management of the employment relationship, the employer can rely on the implied consent of the employees.

So, even if the employees were expressing their lack of consent to the voiceprint program, the Court was willing to go so far as to say that, within the management of the employment relationship, certain uses of employee personal information will be necessary and, in those cases, employees cannot withdraw their implied consent. The court's interpretation of "implied consent", practically speaking, brings PIPEDA in harmony with the PIPA "no consent" model.

Social Media

Another important theme in employee privacy laboratory is the increasingly blurred line between personal and professional life. This is driven largely by our incessant use of social media, where we share intimate details about ourselves, what we do on a daily basis, and our personal views on issues. Of course, many employers seek information on social media as part of the hiring process. In some cases, information shared on Twitter, on blogs, and through unrestricted social network profiles can be easily found through a Google search. Where information isn't as broadly available, the search may escalate to using profiles on social networks to connect with, and learn more about the potential employee.

In May 2011 our office issued *Guidelines for Social Media Background Checks*. This document provides helpful guidance on some of the legal considerations

that employers must bear in mind when conducting social media background checks. For example, employers accessing social media may be collecting personal information that is inaccurate, and are likely to collect information that is unrelated to the job at hand—information about the prospective employees' friends and family, political views, race and sexual orientation. Furthermore, while private sector employers can request consent, public sector employers must be able to demonstrate that the collection is necessary for an activity of the public body, or if it is otherwise authorized, even if they already have an individual's consent.[1]

Since we issued those guidelines, we have seen reported instances of US employers demanding potential employees to provide Facebook login credentials as part of the hiring process. Not surprisingly, these cases were widely condemned by privacy advocates and the media. Facebook publicly stated that requesting employee passwords is "not the right thing to do".[2] California, Delaware, Illinois, Maryland, Michigan and New Jersey responded swiftly by passing laws that prohibit employers from demanding social media passwords from current and prospective employees.[3] Many other states have introduced similar bills.

Not everyone agrees that employers should be prohibited from requesting social media passwords though. The various laws introduced in the United States have been opposed by industry groups in the financial services sector who claim that employers have a right - or possibly even an obligation - to monitor the information that employees may be sharing through social media. While I can't comment on the legality of a hypothetical situation, I can say that it is difficult to contemplate a scenario in which BC privacy law would authorize a public or private sector employer to require an employee to provide a Facebook password.

In fact, we have had the occasion to look into one instance of this when the B.C. NDP party asked candidates running for the leadership of the party to provide officials with their Facebook credentials. Some candidates consented (perhaps reluctantly) but at least one refused to provide his password. This prompted an investigation by our office and we ultimately concluded that the NDP had violated PIPA by collecting the candidates' passwords.

Our analysis into the NDP matter relied heavily on an often overlooked, but extremely important, tenet of our privacy laws. I'm talking about the overriding "reasonableness" standard. In BC, this principle states that "in meeting its responsibilities under the Act, an organization must consider what a reasonable person would consider appropriate in the circumstances".

---

[1] http://www.oipc.bc.ca/tools-guidance/guidance-documents.aspx
[2] https://www.facebook.com/note.php?note_id=326598317390057
[3] http://www.nbcnews.com/technology/new-state-laws-ban-employers-getting-your-facebook-password-1C7785092

Consent is not the silver bullet. This provision is extremely important because even if an employer obtains the consent of a prospective employee to use their Facebook password, I can't see how a reasonable person would consider it a legitimate use.

Related to the issue of social media background checks is the more traditional, but heavily relied upon, criminal records and police information checks as an employment screening tool. Here, the same principles apply so it won't be sufficient for an employer to rely only on consent.

Police Information Checks

I can't say too much on this particular topic because my office is currently investigating the use of police information checks by both the private and public sectors in British Columbia. Safe to say, I think it's important to emphasize the sensitivity of the information employers are collecting through these processes. This is especially the case for police information checks because these reveal a variety of details about an individual's interaction with the police that may not have been proven in court, *e.g.,* investigations that did not result in charges, charges that did not result in convictions, and information relating to a suicide attempt or mental health intervention. This is undoubtedly information valuable in the law enforcement context but opening up non-conviction records for employment screening may be a repurposing of the data.

BYOD

Another issue that's posing challenges for employers is the growing trend for staff to use their own mobile devices in the workplace. This is commonly referred to as "bring your own device", or BYOD.

BYOD raises some significant privacy challenges. On the one hand, employers have an obligation to ensure that devices used for work purposes are trustworthy and secure. Countless data breaches are due to lost or stolen mobile devices. However, efforts by employers to control and secure employee-owned devices can have considerable implications for employee privacy.

Mobile devices such as smart phones and tablets can contain a significant amount of personal information, including photos and other files, email, text messages, browsing history, and location data. Much of this information is sensitive, and employees do not expect that it will be accessed by employers. The fact that the BYOD trend is driven, at least in part, by employees who want to use their own device in the workplace shouldn't mean that employees are required to forgo all privacy rights in their mobile devices.

Last year, in *R. v. Cole*, the Supreme Court found that a teacher had an expectation of privacy in files he had stored on a laptop owned by his employer, the school board. Although the school board had given staff explicit permission to use laptops for personal use outside of school hours, the Supreme Court stated that an expectation of privacy could arise where personal use is "reasonably expected."

Although this case involved s. 8 of the *Charter or Rights and Freedoms* and arose in a criminal context, it was an important pronouncement on the rights of employees with respect to personal information on computers and mobile devices. If employees can expect privacy in employer-owned devices, then undoubtedly they should have an expectation of privacy in their own devices used for work purposes.

What does this mean for employers?

First, consider the fact that employees may already be using personal devices for work purposes, regardless of whether it is formally permitted. With this in mind, it is important to get out ahead of the issue with a proactive BYOD policy. Employers that choose to allow BYOD must ensure that security considerations are balanced with employee privacy.

Consider technical solutions that allow personal information to be stored and accessed separately from employer-owned information. I would be remiss if I didn't acknowledge an important decision handed down by the Supreme Court of Canada on November 13, 2013, in a case about privacy rights in public spaces, and the balancing of privacy with freedom of expression.

In a unanimous decision, the court declared Alberta's *Personal Information Protection Act* invalid because it violated the *Charter* by restricting a union's ability to photograph and post images of people crossing a picket line. *Alberta Information and Privacy Commissioner v. United Foods and Commercial Workers*,[4] is another first in its examination of the balance between personal privacy rights and freedom of expression in the context of labour relations.

The court found PIPA invalid in this narrow context, and gave the Alberta Legislature 12 months to decide how to make the statute constitutionally compliant. Privacy Commissioners and advocates across the country are somewhat reassured because the decision includes very strong statements about the importance of privacy in the digital age, and its quasi-constitutional underpinnings. Others are reading the decision in a broader light—some are celebrating the decision as a general victory for expressive rights beyond the labour environment, *e.g.,* in the commercial and law enforcement contexts.

[4] http://scc-csc.lexum.com/decisia-scc-csc/scc-csc/scc-csc/en/13334/1/document.do

I read the decision narrowly—the Court found that the Unions' interest in freedom of expression outweighed the privacy interests of complainants in this case. The decision will very likely have an impact on the BC PIPA law (its language is very similar), and perhaps PIPEDA and the Quebec private sector law. I have begun discussions with our Ministry of Justice about the BC implications but there is no reason to expect that *Alberta v. UFCW* will lead to a litany of successful challenges based on freedom of expression. A union's right in this context is a well-established right under Canadian law.

I'd like to close by emphasizing that the employment laboratory for privacy issues is only going to get more complex and challenging. While we have already tackled technologies such as GPS, voiceprints, and smartphones, this is just the tip of the iceberg.

Technology

Every day, new technologies are invented and brought to the forefront and many of these inventions involve the collection of massive amounts of personal information. On the horizon will be an increased use of biometrics in the workplace as we continue to learn about the science of authentication techniques. Couple these technologies with the plethora of new sensor devices that can track our movements, the speed at which we are moving and then measure that against our heart rates or blood sugar levels—and we can only imagine what issues we will have to tackle in the workplace privacy lab.

I say all of this without even getting into details about what's going to happen in the very near future when the colleague sitting in the cubicle next to you shows up at work wearing Google Glasses.

I am not fearful of the future, but I do think it will be challenging. And, on that note, I want to stress that employee privacy is much more than a legal issue.

Trust

A successful employee-employer relationship is about trust, collaboration and mutual respect, and the use of privacy-invasive technologies or practices can significantly undermine that relationship. Disputes and complaints may be unavoidable in some cases, but in many others, the fact that an employer is engaged in a drawn out legal battle means that you have already lost.

It's essential that employers think carefully before engaging in new practices that will affect employee privacy, regardless of whether a given collection or use may be authorized by legislation. It's important to keep in mind that people don't give up their rights just because they show up at work.

Lastly, employers must consider whether the potential benefits will outweigh the impacts on employee privacy. Otherwise, your organization, or your client's organization, may find itself under a regulator's microscope.

If you'd like to know more about our office, visit our website at www.oipc.bc.ca or follow us on Twitter at BCInfoPrivacy for the latest updates.

I'm happy to answer any questions you have.