OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Commissioner's January 18, 2011 keynote address to the Western Canada Labour Relations Conference

SOCIAL NETWORKING IN THE WORKPLACE

Thank you for that kind introduction.

I know that the title of my keynote is supposed to be 'Trends in Employment Privacy', but the organizers have given me license to deviate from the agenda and what is very much on my mind these days is social networking!

I have deep experience in examining social networking sites – Facebook in particular – in terms of user privacy. I led the team at the investigation and made the finding in the Federal Privacy Commissioner's office in 2009 when I was Assistant Commissioner. So I hope you will indulge me and allow me to share with you my thoughts on social networking in the workplace. As I am the luncheon speaker, and because this topic will be discussed at a panel tomorrow, I promise not to dive deeply into the case law. You can enjoy your dessert!

Introduction

The explosion in the popularity of social networking sites on the internet has transformed what we are able to know about each other! There are now about 200 major social networking sites worldwide and several boast tens of millions (or in the case of Facebook) hundreds of millions of users.

Social networks themselves are a relatively new phenomenon. So, the topic of how these networks are transforming our workplaces is particularly fresh and we are only beginning to understand some of the implications.

I am speaking to you today about how sites such as LinkdIn, Facebook, MySpace and even YouTube are having an effect on the way people work and on the way employers manage their employees. From cradle to grave, or from recruitment through to termination, it seems that social networks are playing a significant and new role in the employment relationship.

Social Networks: Some basics

- Social networking sites can be a very efficient way to connect. They help us to keep up with friends, share ideas with colleagues in our fields of work, and trade information with people who share the same hobbies and interests. They can be used for project collaboration, event organization or public outreach.
- They are a web-based service that provides a way for users to interact with an online community or network of people with a common interest. They allow individual users to construct a personal profile within the website, specify a list of other users with whom they have a connection, and view their list of contacts in addition to the contacts of other users on the site. Usually, the site will allow individuals to interact with one another using email, instant messaging services or file sharing
- Around the world, active Facebook users double every six months, and in October there were a reported 600 million users worldwide. Nine in 10 young Canadians now regularly socialize online.
- These sites have become an indispensible tool for professionals to keep up with their subject expertise. In fact, you run the risk of becoming out of date if you don't follow and participate in online discussions.

Digital Divide

Social networking sites are viewed differently according to age and generation. It is another example of a digital divide.

The point was made clear in research conducted at Ryerson University's Privacy and Cyber Crime Unit. After speaking to both young people and employers, researchers found a major disconnect between a generation of young Canadians and a generation of managers and executives for which young Canadians work.

The primary difference is that young Canadians believe in "network privacy". This is the notion that the information they post is private because it is posted for the benefit of the individual's own social network.

But organizations believe that information posted online is public and deserves no protection!

And lastly, the research tells us that – for the most part – organizations do not yet have policies, practices or guidelines in place that explicitly govern the use of online social networks by their employees.

Social Networks – Changing the workplace

Privacy in the workplace is itself a topic that is still in its infancy. The added complexity provided by throwing social networks into the mix places the issues of workplace privacy further into disarray.

In the world before social networks, disgruntled employees would vent to one another – perhaps on the shop floor or in the nearest coffee shop. However, today, workplace complaints are sometimes aired online. And people's perspective of what is publicly available and what is private has created a new kind of so-called digital divide. The result: the workplace complaint is now aired more widely – in front of co-workers, clients, suppliers and other third parties.

The net result is that there is a real potential of damage to the reputations of organizations and people.

We now have an English word to describe being fired for an online activity. The Macmillan English dictionary defines the word "dooced" as "having lost your job because of something you have put in an internet blog". The term was coined by a Los Angeles web designer who lost her job after writing about work colleagues in her personal blog.

As recently as last October, the B.C. Labour Relations Board ruled that an employer had good cause to fire two employees who made "disrespectful, damaging and derogatory comments on Facebook".

While this may have been the first case in B.C. dealing specifically with posting on Facebook, it's clearly not going to be the only one. In fact, we are already seeing more and more examples. A grocery chain in Ottawa (Farm Boy) also fired several of its young employees after they posted derogatory comments about the stores and its customers. And Starbuck's fired an employee in Toronto after the employee criticized his superior on Facebook after the worker was prohibited from going home sick.

These are a few examples of actual firings. To be clear, there are already many examples of people who have been disciplined for inappropriate postings to social networking sites. In B.C., a principal got into trouble after posting naked holiday photos of himself to the internet. The mother of a student at his school had stumbled across them and took offence.

Recruitment

Profile pages on networking sites contain a wide range of personal information which can be accessible to all depending on an individual's privacy settings. As well as

standard background information on profile pages, photographs and voluntary information such as political preferences, religion, relationship status, sexuality and interests can be posted. Individuals can post information and access information about others.

Employers are increasingly searching social networking sites as part of their recruitment vetting process. One "feel good" story appeared recently in the New York Times.

Alan Kennedy, 54, had never used social networking sites until he was laid off from his job as an engineer last November. Then he did what many job seekers are now advised to do: he set up profiles on Facebook and LinkedIn.

In March, after several depressing months of searching, Mr Kennedy received a "Jobvite", an email invitation to apply for a job. The invitation came from a former co-worker who had gone to work for a software company that was offering bonuses to its employees to help fill them.

Mr. Kennedy's former co-worker used a software tool to search the profile information of his Facebook friends and LinkedIn contacts. He flagged Mr. Kennedy as a possible match to a job listing. Mr. Kennedy responded to the invitation and within a week was working as a software engineer there. "I landed a job I might never have heard of otherwise".

But it is not all good news. Research by recruitment firms and Microsoft in December 2009 has shown that individuals have failed in job applications due to information set out in the social networking profile pages.

Employers need to ensure that recruitment decisions based on the content of networking sites do not render them liable for violating the law! To avoid potential liability, best practice would dictate that an applicant be informed about the vetting and verification exercise and given an opportunity to comment on the accuracy of the information collected.

And since employers are undoubtedly using social networks as a way to perform background checks on candidates, individuals must also be vigilant in what they post.

This warning is particularly apt considering that once information is posted online, it takes on a "permanence' of its own. It is not always that easy to undo the damage done by posting pictures of your New Year's Eve party because simply trying to take them down doesn't mean that they were not otherwise viewed, saved, and cached.

Workplace Monitoring

A related issue is the monitoring of how much time employees spend looking at social networking sites while at work. Productivity issues are obviously a concern to organizations.

Some surveillance in the workplace is required and is acceptable. Employers have the right to know whether workers are doing the job they are paid to do. But workers do not check their privacy rights at the office door. Workplace privacy is an important part of the basic autonomy rights of individuals. And when workers are expected to be more and more accessible during off-hours with mobile devices, the lines between work time and personal time can become increasingly blurred.

When it comes to monitoring, we know that there is a four-part test that commissioners and the courts have used to determine if a private sector employer's actions are reasonable. The test asks:

- Is the monitoring demonstrably necessary to meet a specific need?
- Is the monitoring likely to be effective to meet that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy intrusive way of achieving the same end?

If employers do monitor the sites employees are looking at and how much time they spend there, then the employer should tell the employees that they are watching and what triggers the surveillance.

A related issue is that social networks are now increasingly encouraging users to post geo-location data. So, information about an employee's location while supposedly away from work because of illness is something that can now be obtained with relative ease compared to the old-fashioned way of, for example, hiring a private investigator to follow the employee. But, just because it's now easier to monitor employees' locations does not mean that it is always permitted.

Legal Issues

While the adoption of social networks in the workplace can be a great innovation, it is important that employers who contemplate it keep in mind certain legal requirements.

There will be different legal requirements depending on the context. For example, requirements might be different if the social network is an "internal' network created by the employer as opposed to using an existing "publicly available" platform such as Facebook or LinkedIn.

Another factor to consider is whether or not you operate in the private sector as opposed to the public sector.

For private sector organizations, as I stated earlier, you must consider when it is appropriate to collect personal information when recruiting or monitoring employees.

For public bodies subject to B.C.'s FIPPA, they must make sure to abide by the general legal requirement that personal information remain and be accessed ONLY in Canada because of the restriction on trans-border data flow of personal information. This might be a difficult requirement to meet in some situations, particularly if the social network stores information in the cloud.

Also, public bodies must remember that information posted to social networks are subject to the "access" provisions of FIPPA as well. So, figuring out how to respond to access requests for information on the networks is an important consideration to keep in mind as public bodies begin to embrace the use of social networks in the workplace.

And training is important here too. If the public is so used to revealing everything on a social networking site, this can create a risk for the public body that is considering creating an in-house social network for the purpose of sharing or working more horizontally, because the information posted is likely an accessible record which, taken out of context, could lead to problems for the public body. Training or what is appropriate behaviour and ground rules of communications on blogs, social networking sites, etc. are also important.

Need for policy and dialogue

While many employers have guidelines and codes of conduct for email and internet use, social networking sites pose different privacy challenges which should be specifically addressed in conjunction with these other workplace rules. Clear rules and policies drafted specifically on the use of social networking should be communicated to all employees.

The policy should generally establish best practices and outline expectations for acceptable use of social networks in the workplace, set out the consequences of misuse, and address any workplace privacy issues. A key ingredient to the successful use of social networking in the workplace is a health and transparent dialogue between employer and employees.

Conclusion

I advise employers to act extremely carefully. The decision by an employer to collect information about a current or potential employee from a social networking site will

depend on a number of contextual factors dependent on the unique circumstances of each case.

The first step is to recognize that you are collecting personal information, and therefore you must look carefully at what privacy law applies to your organization. There will be unique requirements that apply.

Secondly, you should ask yourself why you are collecting this personal information. As part of this analysis, private sector employers should be able to establish why a reasonable person would consider it appropriate in the circumstances to collect this information via a social networking site.

Public sector employers should consider whether other, less invasive, less indiscriminate and more reliable means of collecting personal information are available.

I would like to leave you with this an excerpt from article I read recently:

Clark and Roberts, authors of an article on Employer's Use of Social Networking Sites: A Socially Irresponsible Practice, articulate well the difference between traditional methods of collecting information about employees and collecting information using social networking sites:

The difference is that the digital information becomes permanent and employers are being the voyeurs. Employers are taking in all kinds of personal information, and making decisions based upon that information, without job applicants being aware. Employers are doing so because it is easy and cheap to do so. We contend that an employer would not ask a human resources staff member to follow a job candidate to a local restaurant or bar and sit in the booth beside him or her for the purpose of overhearing conversations and witnessing behaviour for a character check. As long as the job candidate is in a public place, the employer could do so, but for most this action would seem extreme and inappropriate. Why do we not have a similar reaction when the same behaviour occurs online?

Our office is working on guidelines for social networking in the workplace. I plan to consult with key stakeholders in the coming month. Stay tuned.

Thank you for your attention this afternoon.

Questions ?