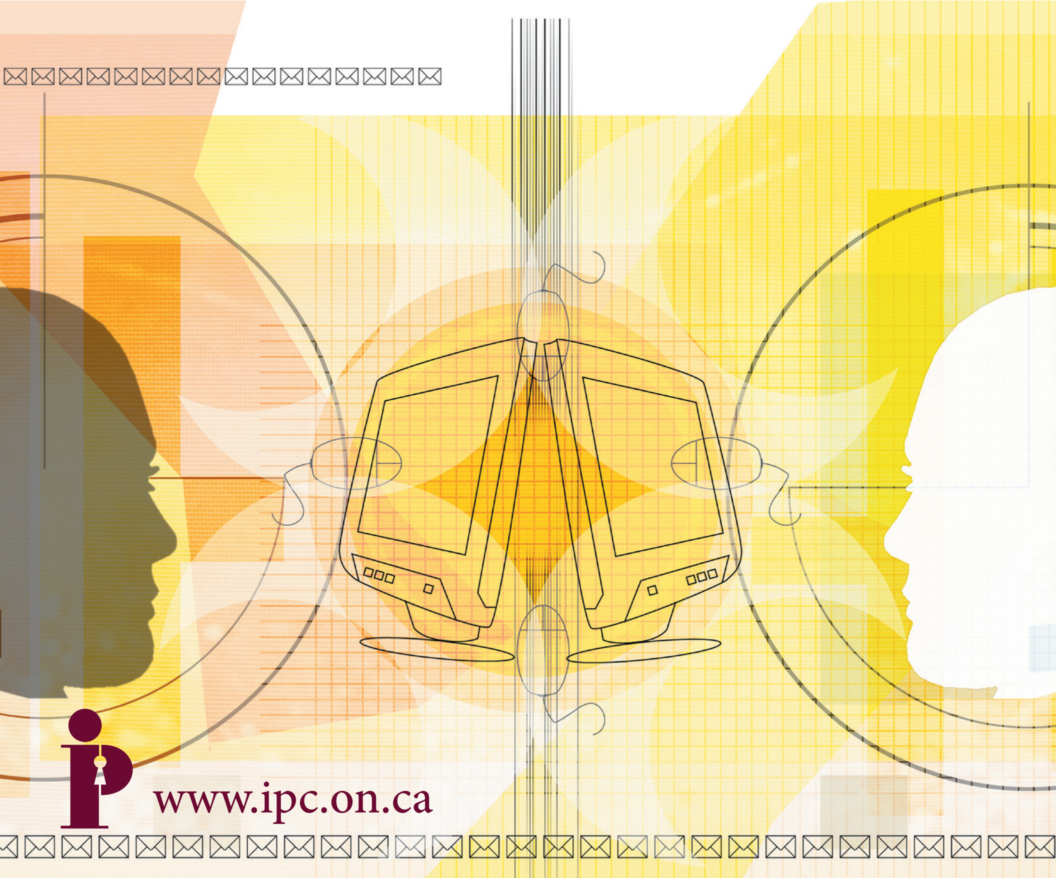
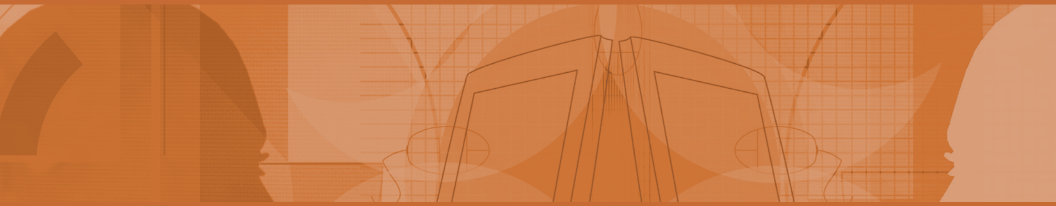
Reference Check: Is Your Boss Watching?

Privacy and Your Facebook Profile



www.ipc.on.ca



Reference Check: Is Your Boss Watching?

Privacy and Your Facebook Profile

Facebook and other online social networks are the Web destinations of choice for more and more people to connect, communicate and share personal information with others.[1] While they may have initially started out as networking and recreational tools for young people, online social networks now attract people of all ages.[2]

The practice of employers looking for background information about job candidates on social networking websites such as Facebook has grown dramatically.[3] These sites along with search engines are now being used as a business tool by human resources departments to perform background checks on potential employees. Users of Facebook and other such sites should post information with their eyes wide open — considering the risks to their employment prospects, current and future. This paper provides important information and suggests ways of mitigating and minimizing such risks.

It is crucial to remember that anything posted online may stay there forever, in one form or another. Whether through the Internet Archive's Wayback Machine site,[4] or the caches of Google and Yahoo, old versions of websites are indeed searchable by those in the know. What is actually found may include your own posted material, as well as information about you posted by others. This uncertainty regarding one's privacy and confidentiality of sensitive information is a major downside to social networking sites, despite their many positive aspects. Anything associated with you – or the people you are connected to – can, and most likely will, be viewed and evaluated by other people, some of whom may have considerable influence over your life, now or well into the future.

When you realize that information about you on the Internet may be used in a work-related context, you may see things in a different light. Depending on what information is posted, it could seriously harm, or help, your prospects. Users of sites such as Facebook, Google, LinkedIn and Twitter may feel that anything goes since they are just chatting amongst "friends." This view is sadly mistaken and may have unintended consequences. Consider the following:

> January, 2007 – Farm Boy, an Eastern Ontario grocery chain, fired several employees from its Ottawa store after learning of the content of postings on a "I got Farm Boy'd" group on Facebook. A former employee was quoted in the *Ottawa Citizen* as saying that he was accused of stealing from the store, based on his posts on the group's page.

And it is not only current employers who may be looking at your network content. A potential employer might find certain material offensive or even troubling, and may decide not to interview you. They might even see or read things they would not be allowed to ask you about in an interview, due to human rights laws. Recruiters can – and do – use search engines and social networks to gather background information on job candidates, and many are beginning to eliminate candidates based solely on what they find online. Facebook has made this even easier by allowing limited member profile information to be searchable on public search engines, but members can prevent this by using their privacy controls.

Another common practice that is occurring in the United States is for employers to ask job applicants to "friend" a human resources staff member or to log in to a social network using a

company computer during an interview so the employer may review their online activities. Some employers have gone so far as to ask candidates to provide them with their username and password.[5] This intrusive practice has put many people in the difficult position of having to choose between obtaining employment and disclosing their usernames, passwords and the intimate details of their lives . Facebook's Chief Privacy Officer Erin Egan in a posting on their blog expressed her company's opposition to this practice and stated that, "this practice undermines the privacy expectations and the security of both the user and the user's friends. It also potentially exposes the employer who seeks this access to unanticipated legal liability."[6]

Fortunately, this does not appear to be the case in Canada where human rights and privacy laws provide stronger protections for job applicants. Employers cannot ask for information that may directly or indirectly reveal a prohibited ground of discrimination. In Ontario, requests for this kind of information may also put the employer at risk of a lawsuit as an unreasonable intrusion into not only an applicant's private activities, but also the activities of their 'friends'.[7]

If employment decisions about you were made based on information obtained from social networking websites, you may never know why you didn't get the job, the interview, or the promotion. At least for now, those decisions are likely being made by individuals for whom the "tell-all" nature of Web 2.0 tools, like social networking sites, still seems foreign, embarrassing, risky, or even seriously misguided in the business world.[8] What *you* might see as fun and meaningless in a "Wall" post or photo could be interpreted as evidence of recklessness

Here are a few examples of the types of entries that might raise concerns for employers doing research on you:

- Questionable recreational activities captured in photos on your profile and your friends' profiles. For example, if you appeared drunk or out of control, "partying" or otherwise engaged in behaviour that may be considered offensive, your reputation could suffer.
- Your comments about employment situations:
  - "I hate my boss!"
  - "I was late for work again today. I just can't get out of bed!"
  - "I shouldn't have to work so hard!"
- Your religious, political, or sexual activities or views (stated or implied through membership in groups).

and lack of judgment by someone who doesn't understand the context. Your activities, comments and views, even though you may only have been joking around with your friends, all become part of an online résumé that, inadvertently or not, becomes available to everyone.

What can you do to protect yourself – to avoid embarrassment and worse, loss of employment opportunities?

1. "Think hard before you click" to post text or photos to groups or discussion boards or write on anyone else's pages, in ways or on topics that you would not want to discuss with your current employer, or in a job interview. Inappropriate, demeaning or defamatory comments related to your work are particularly risky.

2. Review what is out there about you, on social networking sites, on customized business and HR sites such as ZoomInfo and LinkedIn, and through search engines such as Google. Some of it might be completely fictional. Others may be referring to someone else with the same name as you, but you need to know about it.

3. Remove, if possible, anything you would not want to discuss with your current employer, or in a job interview; ask friends to take down items such as questionable photos of you. There are now private services available, such as reputation.com (www.reputation.com) that can be retained to do this for you.

But you should be aware that the effects of some information may continue:

- information removed could still live on in cached or archived copies of the website, which may be located by Internet users who are determined to find them. Be prepared to explain any of the deleted material;

- it will be almost impossible to have material removed that has found its way into news media or government records;
- damaging information may have already been viewed by potential employers.

4. Implement strong privacy controls over your personal information on online social networks. Start by reviewing your privacy settings. These may be tricky to use, so once you've set them up, make sure you test them out – have someone try to look at your profile, or search it yourself on a public search engine.[9]

- remember that if viewers of your profile can also view your friends' pages, they may see images and read remarks that you'd rather they did not. You should also ensure that your profile is not visible to viewers of friends' pages, and if possible, apply appropriate privacy controls – Facebook has several – to ensure that photos of you on other people's pages are not 'tagged' with your name.
- be extra careful with applications created by third parties within social networks. These applications may collect your personal information, and unless you find and agree to their privacy policy (and they adhere to it), you may have no idea what might be done with that information.

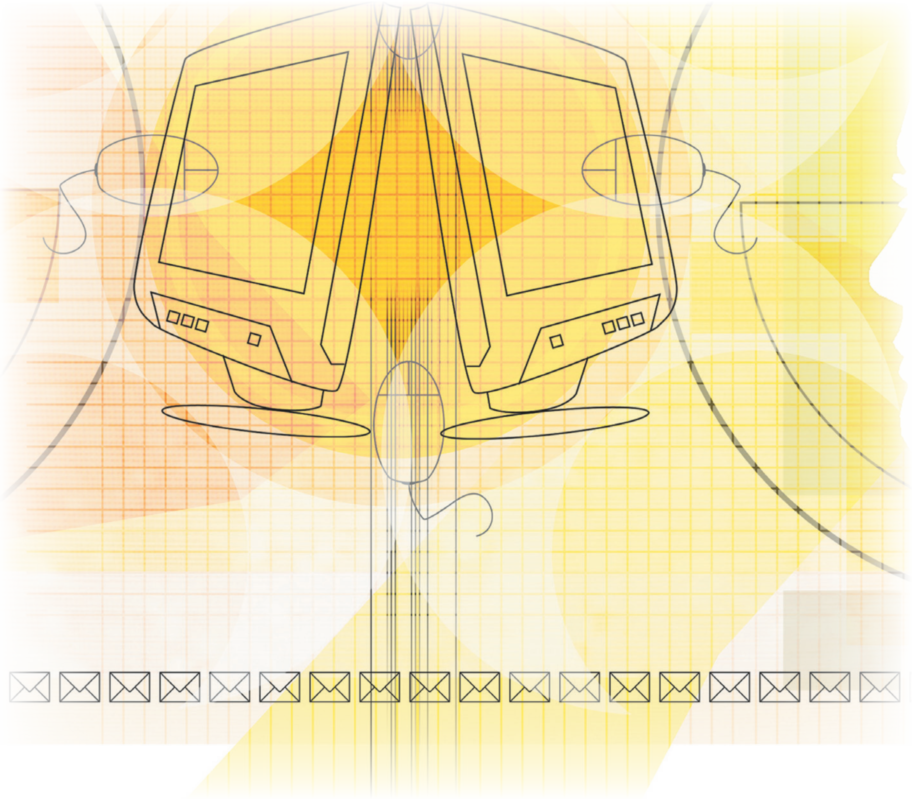
5. Educate yourself about your rights in various areas – under employment, human rights and privacy laws. Consider very carefully any request from a prospective employer requesting access to your password protected social media sites – they shouldn't be asking.

6. Build up a positive image for yourself on your profile through comments on your own and others' sites, photos, and groups – that's what you want prospective employers to see.

7. Keep it factually accurate – employers may engage in fact-checking with others or reach out to additional sources.

Conclusion

We have to say it again, but it bears repeating – the Internet, the Web – is a fundamentally public place. If you can't get rid of something, you must assume that it's going to be seen, so get ready to explain it. Better still, think before you post!



Endnotes

1 According to a January 2012 report by comScore, social networking sites now reach 82 per cent of the world's online population (1.2 billion users), nearly 1 in every 5 minutes spent online is now spent on social networking sites (6.7 billion minutes), with Facebook having a global reach of more than 800 million users. http://bit.ly/wzLFoY

2 A July 2011 Ipsos Reid poll found that 60 per cent of all Canadian Internet users had a profile on a social networking website, with the vast majority – 86 per cent having a Facebook profile. This includes 43 per cent of online Canadians over the age of 55. http://bit.ly/nnDhvk

3 In survey data from ExecuNet, 90 per cent of recruiters used Web search engines to research candidates and 46 per cent said they had ruled out candidates on that basis. ExecuNet also notes, however, that 80 per cent of recruiters said a candidate's job prospects improved when positive information was found online. ExecuNet Executive Insider March 2010, republished at http://bit.ly/btOcgy

4 http://www.archive.org/web/web.php

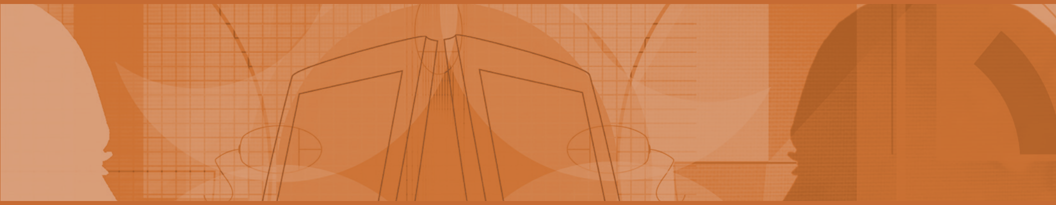
5 See Job seekers getting asked for Facebook passwords by Manuel Valdes and Shannon McFarland of the Associated Press, March 20, 2012. http://yhoo.it/GAXAzY

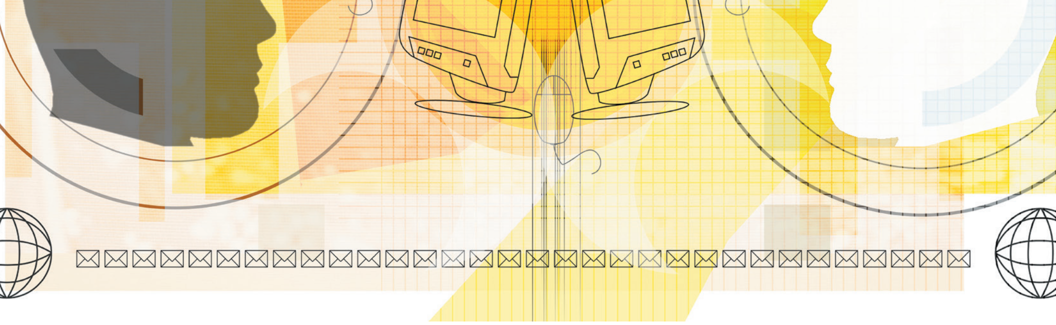
6 On March 23, 2012 Erin Egan, Chief Privacy Officer, Policy at Facebook posted Protecting Your Passwords and Your Privacy on the company's blog. http://on.fb.me/GUtWT1

7 In January 2012 the Court of Appeal for Ontario recognising invasion of privacy as an actionable tort in Ontario under the tort of 'intrusion upon seclusion', and awarded damages to the plaintiff. http://bit.ly/A2NBUk

8 See John Palfrey's comments about "digital natives" and "digital immigrants", HBR Case Commentary, Harvard Business Review, June 2007, p.42.

9 Do not rely absolutely on these controls; they may change without your being informed.





About the IPC

The role of the Information and Privacy Commissioner is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

For more information:
Information and Privacy Commissioner
Ontario, Canada

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 CANADA

Tel: 416-326-3333 or 1-800-387-0073
Fax: 416-325-9195 TTY: 416-325-7539
info@ipc.on.ca www.ipc.on.ca

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC® C017307

Cette publication est également disponible en français

Updated: July 2014