Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile

February 2009

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 started out as networking and recreational tools for young people, the large 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 is also growing.[3] These sites are now being used as a business tool by hiring managers who see their potential, along with search engines, for 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 will suggest ways of mitigating and minimizing such risks.

It's crucial to remember that **anything posted online may stay there forever, in some 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 who know how. What is actually found may include your own material, as well as information *about* you, posted by others at other sites. 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 in 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

1 According to comScore, considered the global leader in measuring the digital world, Facebook became the largest of the top 10 *gaining* properties in terms of monthly unique visitors, in May 2007, with at least five times more visits per visitor than any of the others in the top 10 fastest growing sites.

2 A recent Canadian poll of Internet users found that one-third of online Canadians aged 50 and over have visited social networking sites. For those in their 40s, it's 45%. **http://www.newswire.ca/en/releases/archive/June2007/11/c2653.html**

3 In survey data from ExecuNet, 77% of executive recruiters used web search engines to research candidates and 35% said they had ruled out candidates on that basis. **http://www.execunet.com/m_releases_content.cfm?id=3349** and **http://www.execunet.com/m_releases_content.cfm?id=3503**. ExecuNet named "job search buried by digital dirt" as one of its top five employment trends for 2007.

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

information is posted, it could seriously harm, or help, your prospects. Users of mass-market sites such as MySpace, Facebook and Friendster may feel that anything goes and "free speech" should prevail since they are just chatting amongst "friends." And they may feel that as part of a closed network – a school or a geographic region, they have some built-in privacy protection. Both views are mistaken.[5] 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 page.

And it's not only current employers who may be looking at your network content. It's your potential future boss, or someone who might never become your boss if he or she finds certain material offensive or even troubling, and decides not to interview you as a result. 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 on what they find. (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.[6]) They might see or read things they would not be allowed to ask you about in an interview, due to human rights laws. So if you're going to post sensitive information on your site, you should be prepared to answer questions about any issues relating to your online profile.

Here are a few examples of the types of things that might cause concern and raise questions for employers researching you:

- Your recreational activities captured in photos on your profile and your friends' profiles:
  - If you appear 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!"

5 Facebook networks offer a minimal level of privacy in that profiles of users in other networks cannot be viewed unless they have linked with you as a friend. But it is a simple matter to temporarily join the regional network of a research target in order to try and view that target's profile information, if it is not protected by applying additional privacy settings.

6 See the IPC's tipsheet "How to Protect Your Privacy on Facebook," **http://www.ipc.on.ca/images/Resources/up-1facebk_handout_priv.pdf**

- Your religious, political, or sexual activities or views (stated or implied through membership in groups):
  - If they vary significantly from the mainstream, beware of their potential impact.

If decisions about you are 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 seem foreign, embarrassing, risky, or even seriously misguided in the business world.[7] What *you* might see as fun and meaningless in a "Wall" post or photo could be interpreted as evidence of recklessness and lack of judgement by someone who doesn't understand the context. Your activities, comments, and views, even though you may have just 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 refer to someone 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 Defender (www.Reputationdefender.com) that offer to do this for you, for a fee.

But 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 can be located by Internet users who are determined to find them. Be prepared to explain any of the deleted material;

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

- 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 privacy controls** over your personal information on online social networks. These can 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.[8]
   - Remember that if viewers of your profile can also view your friends' pages, they may see images and read remarks you'd rather they didn't. You should also ensure that your profile is not visible to viewers of your 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.[9]
   - Be extra careful with applications created by third parties within social networks. These applications (such as iLike) may collect your personal information, and unless you locate and agree to their privacy policy (*and* they adhere to it), you may have no idea what might be done with that information.
5. **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.

Finally, 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, assume it's going to be seen and be ready to explain it.

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

9 See the IPC's tipsheet "How to Protect Your Privacy on Facebook," **http://www.ipc.on.ca/images/Resources/up-1facebk_handout_priv.pdf**