

This article first appeared in the B.C. Human Resources Management Association's HRVoice magazine (October 2011).

GUIDELINES FOR EMPLOYERS PERFORMING SOCIAL MEDIA BACKGROUND CHECKS

By James D. Kondopulos of Roper Greyell LLP, Employment and Labour Lawyers.

On October 12, 2011, the Information and Privacy Commissioner of British Columbia issued guidelines to assist organizations and public bodies that use social media sites to conduct background checks in respect of prospective employees and volunteers.

The guidelines can be found on the website of the Office of the Information and Privacy Commissioner (OIPC) by visiting this link:

<http://www.oipc.bc.ca/pdfs/private/Guidelines-SocialMediaBackgroundChecks.pdf>

These guidelines were issued in conjunction with P11-01-MS, a summary of an OIPC investigation which is headed "Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's use of social media and passwords to evaluate candidates" and available online at:

http://www.oipc.bc.ca/Mediation_Cases/pdfs/2011/P11-01-MS.pdf

What is a "social media background check"?

In the guidelines, the OIPC explains what is meant by the term "social media background check":

A "social media background check" can mean many things. It can be as simple as checking out a Facebook profile or as complicated as hiring someone to search for every bit of social media about an individual. The term "social media" ... captures a broad range of information such as social networking sites, blogs, micro-blogging, and file sharing sites ...

The OIPC adds:

There are many ways that employers can search for social media content about an individual. Micro-blogging sites like Twitter have real-time search engines ... and sites such as Google Advanced Search ... filter results by criteria such as domain name and file type.

Employers can search for information from blogs using customized search engines like Google blogs search ...

Risks associated with performing social media background checks

According to the OIPC, there are risks associated with performing social media background checks. Two of the risks identified in the guidelines are the collection of inaccurate information and the collection of irrelevant or too much information:

- (a) ***Collection of inaccurate information.*** Information collected from social media sites may be inaccurate. A social media account belonging to one person may be confused with an account belonging to another person who has the same name. Information collected may be out-of-date or, worse, deliberately manipulated in order to discredit someone. Photographs may be mislabelled. In light of all of this, the OIPC cautions:

Privacy laws require public bodies and organizations to take steps to ensure that the information they collect is accurate. This requirement applies regardless of whether the individual performing the check is viewing information or if they save copies of the information.

- (b) ***Collection of irrelevant or too much information.*** In the view of the OIPC, social media background checks are “[I]ike a dragnet” and “can catch much more than what was intended”. Organizations and public bodies using social media sites to conduct background checks can easily lose control over the amount and kind of information they collect. Information collected may be irrelevant. Photographs may be posted years after they were taken. With regard to the private sector, the OIPC provides this reminder:

Under privacy law, organizations can only collect personal information that a reasonable person would consider appropriate or reasonable in the circumstances ...

There is one other risk identified by the OIPC - the risk of “overreliance on consent”. See, in this regard, pages 3 and 4 of the guidelines.

Guidance when performing social media background checks

In the guidelines, the OIPC provides “some guidance on what to consider when deciding whether to perform a social media background check”.

The “guidance” – which is said by the OIPC to be non-exhaustive in nature – is, for ease of reference, reproduced in its entirety below:

1. Recognize that any information collected about individuals is personal information or personal employee information and is subject to privacy laws, whether or not the information is publicly available online or whether it is online but subject to limited access as a result of privacy settings or other restrictions;
2. Conduct a privacy impact assessment including an assessment of the risks associated with your use of social media as a component of background checks. When conducting this assessment, public bodies and organizations should:
 - a. Find out what privacy law applies and review it, ensuring that there is authority to collect and use personal information;
 - b. Identify the purposes for using social media to collect personal information;
 - c. Determine whether the identified purposes for the collection and use of personal information are authorized;
 - d. Consider and assess other, less intrusive, measures that meet the same purposes;
 - e. Identify the types and amounts of personal information likely to be collected in the course of a social media background check including collateral personal information about other people that may be inadvertently collected as a result of the social media background check;

- f. Identify the risks associated with the collection and use of this personal information including risks resulting from actions taken based on inaccurate information;
- g. Ensure that the appropriate policies, procedures and controls are in place to address the risks related to the collection, use, disclosure, retention, accuracy and protection of personal information;
- h. If the collection is authorized, notify the individual that you will be performing a social media background check and tell them what you will be checking and what the legal authority is for collecting it;
- i. Be prepared to provide access to the information you collected and used to make a decision about an employee or volunteer.

Conclusion

It remains to be seen how all of this will play out in practice.

Suffice it to say, the Information and Privacy Commissioner of British Columbia is quoted in an October 12, 2011 news release as stating:

We enter a new era with the application of privacy laws to social media background checks.

[T]he guidelines my Office is issuing today are designed to provide guidance and practical steps to assist organizations and public bodies in complying with the law.

In the news release, the Commissioner is also reported as saying that she expects organizations and public bodies to “review and adopt the guidelines so that their practices concerning social media background checks comply with privacy obligations”.

James D. Kondopulos practises employment, labour and workplace human rights law at Roper Greyell LLP in Vancouver. He can be reached at jkondopulos@ropergreyell.com. For more information about James' practice and Roper Greyell, visit <http://www.ropergreyell.com/Ourpeople/Jkondopulos.html>.

While every effort has been made to ensure accuracy in this article, you are urged to seek specific advice on matters of concern and not to rely solely on what is contained herein. The article is for general information purposes only and does not constitute legal advice.