Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Guidelines for Social Media Background Checks
October 2011

Introduction

Social media is a relatively new communication medium that continues to transform how we live our lives. However, social media is in its infancy in terms of its legal and policy implications. Like a credit or criminal background check, many employers, volunteer agencies, and other organizations (such as political parties) are now conducting social media background checks on future and prospective employees, volunteers, and candidates. They conduct these checks with and without the knowledge of the individuals they are checking. Currently, there is little guidance from administrative tribunals or from courts about this issue. The Office of the Information and Privacy Commissioner for British Columbia has developed these guidelines to help organizations and public bodies navigate social media background checks and privacy laws.

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.[1] The term "social media" in these guidelines captures a broad range of information such as social networking sites[2], blogs[3], micro-blogging[4], and file sharing sites (including photographs and video).[5]

[1] 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 (twitter.com/#!/search-home) and sites such as Google Advanced Search (google.ca/advanced_search) filter results by criteria such as domain name and file type.

[2] There are now almost 200 major social networking sites. Several boast tens of millions of members. Some networks like www.facebook.com are intended for general social networking purposes. Other niche sites target certain regions (http://mixi.jp), activities (www.couchsurfing.com/), ethnic groups (www.blackplanet.com/) or faiths (http://muxlim.com/).

[3] Employers can search for information from blogs using customized search engines like Google blogs search (www.google.com/blogsearch).

[4] One of the best-known micro-blogging sites is twitter.com with over 200 million users.

[5] Examples of popular file-sharing sites include www.flickr.com and www.dropbox.com.

For many, the concepts of "privacy" and "social media" are inherently at odds, since individuals often post information online about themselves because they want people to see it. When organizations and public bodies search for information about an individual, the collection, use, and disclosure of that personal information is subject to the privacy provisions of BC's *Freedom of Information and Protection of Privacy Act* (for public bodies), or *Personal Information Protection Act* (for organizations).[6] These laws apply whether the individual is applying for paid or unpaid employment, a volunteer position, or if they are applying to run as a candidate in an election.

Putting social media background checks in context

Social media background checks are enticing because they are faster and simpler than other kinds of background checks. Another distinction between social media background checks and traditional background checks is that individuals can perform them under the pretext of a social relationship. These differences can make it difficult to recognize social media background checks for what they are: a tool to screen and monitor current and prospective employees, volunteers, and candidates.

For many, the concepts of "privacy" and "social media" are inherently at odds, since individuals often post information online about themselves because they want people to see it.

Risks associated with social media background checks

Accuracy

Information may be prone to errors, and social media is no exception. The ease with which individuals can link images and information that has been collected from social media to a name, increases the likelihood that the individual performing the check will collect inaccurate personal information. They might guess which social media account matches the name on a resume and screen out a candidate based on incorrect information. In other cases, they might access a social media account that has been set up by an imposter to discredit someone. Other factors that can compromise the accuracy of social media include mislabelled photographs and out-of-date information. Privacy laws require public bodies and organizations to take steps to ensure that the information they collect is accurate.[7] This requirement applies regardless of whether the individual performing the check is viewing information or if they save copies of the information.[8]

---

[6] To read copies of these laws, go to www.oipc.bc.ca.

[7] The accuracy requirement applies to any personal information an employer uses to make a decision about that individual. See either section 30 of the *Freedom of Information and Protection of Privacy Act* for public sector employers or section 33 of the *Personal Information Protection Act* for private sector employers.

[8] See OIPC BC Order P10-01, [2010] B.C.I.P.C.D. No. 7, (Host International of Canada Ltd. (Feb. 10, 2010)) (http://www.canlii.org/en/bc/bcipc/doc/2010/2010bcipc7/2010bcipc7.html).

Collecting irrelevant information, collecting too much information

Like a dragnet, social media background checks can catch much more than what was intended. Individuals performing the checks could collect personal information that might be irrelevant. Under privacy laws, organizations can only collect personal information that a reasonable person would consider appropriate or reasonable in the circumstances. In the public sector, the test is even higher. Public bodies can only collect personal information about an individual if that information relates directly to and is necessary for an operating program or activity of the public body, or if it is otherwise authorized.[9] In addition, as collecting personal information from a social media site is a form of indirect collection, public bodies must have additional authority to collect the information indirectly, such as with that individual's consent.[10]

With other forms of information gathering, organizations and public bodies have greater opportunities to control the amount of information they collect. For example, an employer would normally ask references about a job candidate's work habits but not about their marital status. With social media background checks, they can quickly lose control over the quantity of information they collect about an individual.

Like a dragnet, social media background checks can catch much more than what was intended.

Similarly, public bodies and organizations have little control over the currency of the information they collect from social media. Someone might post photographs of an individual on a social media site that are several years old. In addition, many social networks make information available indefinitely. With other forms of background checks, individuals performing screening are usually able to specify in advance if they only want to see personal information from a certain period.[11]

Overreliance on consent

It is problematic for public bodies or organizations to rely on consent to perform a social media background check for a number of reasons.

[9] Public bodies may also collect personal information if the collection is expressly authorized by an enactment or if that information is collected for the purposes of law enforcement. For the precise wording of the statutory requirements, public bodies in BC should refer to section 26 of the *Freedom of Information and Protection of Privacy Act.*

[10] Consent is not the only authority for public bodies to indirectly collect personal information. For a complete list, public bodies should refer to section 27 of the *Freedom of Information and Protection of Privacy Act.*

[11] Using date range filters on search engines does not address the problem of filtering the currency of information online. This is because an individual (or their friend) might post a photograph years after it was taken.

Under private sector privacy laws, organizations could ask an individual for consent to access their social media content; however, privacy laws usually permit them to withdraw their consent at any time. If they withdraw it, the organization must not use that information to make a decision about that individual.[12] One exception to this is in circumstances where an employer finds social media content that is about that individual's employment (including volunteer activities). In these circumstances, they may be able to use that information without the individual's consent if it is for reasonable purposes relating to recruiting or establishing, managing or terminating the employment or volunteer relationship. For example, if an employer sees a Facebook posting by an employee that contains proprietary company information about a new product, the employer could likely use that information without the employee's consent.[13]

It is problematic for public bodies or organizations to rely on consent to perform a social media background check for a number of reasons.

Public sector employers cannot collect personal information from social media sites unless it is necessary for an operating program or activity of the public body, or if it is otherwise authorized[14], even if they already have an individual's consent.[15]

A separate problem is the inadvertent collection of third-party personal information. For example, if an organization obtains consent from an employee or volunteer to retrieve a video on Facebook that he says proves he did not start the fistfight at the company picnic, the organization will likely be collecting personal information (without consent) about whoever did start it. If this individual is an employee or volunteer, they might be able to collect that information even without consent. If the instigator turns out to be someone else, then that organization has likely collected personal information without proper legal authority.[16]

---

[12] In addition, under private-sector privacy laws, even if an individual gives consent for an employer to access their social media content, the collection must still be reasonable. For example, if a job applicant gives an employer permission to access her online dating profile, this would likely still contravene private-sector privacy laws because collecting that information would not be reasonable in most circumstances.

[13] Since most information on social media sites is not about an individual's employment, it would not fall within the definition of "employee personal information" in the *Personal Information Protection Act*. Public-sector privacy laws do not distinguish between information about employees and other types of personal information.

[14] Public bodies may also collect personal information if the collection is expressly authorized by an enactment or if that information is collected for the purposes of law enforcement. For the precise wording of the statutory requirements, public bodies should refer to section 26 of the *Freedom of Information and Protection of Privacy Act.*

[15] Public bodies should see footnote 10 for more information on indirectly collecting personal information.

[16] Public sector employers can collect personal information if it is necessary for an operating program of the public body, if it is expressly authorized under an Act, or if the information is for the purposes of law enforcement, which includes non-police investigations that could lead to a penalty or sanction.

What to consider

Below is some guidance on what to consider when deciding whether to perform a social media background check:[17]

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.

[17] This guidance is non-exhaustive. Employers should evaluate the entirety of the legislation that applies to them whenever they collect, use or disclose personal information. For example, employers should always determine how long they are required to retain personal information and should establish a process to correct inaccurate personal information, when appropriate.

Organizations and public bodies must only perform social media background checks if they can demonstrate the proper authority.

What to avoid

Here is what public bodies and organizations should **not** do when deciding whether to perform a social media background check:

1. **Wait until after they conduct a social media background check to evaluate compliance with privacy legislation.**
2. **Assume in advance that a social media background check will only retrieve information about one individual and not about multiple individuals.**
3. **Perform a social media background check from a personal account in an attempt to avoid privacy laws.**
4. **Attempt to avoid privacy obligations by contracting a third party to carry out background checks.**
5. **Perform a social media background check under the assumption that individuals will never be able to find out about it. For example, an individual could use web analytics to try to determine what IP address accessed their personal information.**

Once collected, information can be very difficult to disregard. If an individual suspects that their personal information was improperly collected, they have a right to complain to the Information and Privacy Commissioner.[18]

[18] In addition, individuals can complain if they believe that an employer has not adequately responded to their request for access to their personal information or if an organization or public body has failed to correct their personal information. In the case of private-sector employers, individuals can also complain to the Commissioner if they believe that an organization or public body has failed to respond adequately to questions about how they have used and disclosed their personal information.

The role of the Information and Privacy Commissioner

The Information and Privacy Commissioner has statutory authority to investigate compliance with privacy laws.[19] The Commissioner can require public bodies and organizations to respond to questions under oath about how they have collected, used or disclosed personal information. If the Commissioner determines that an organization or public body has violated privacy laws, the Commissioner can issue an order compelling them to take remedial action. In some circumstances, an individual affected by a Commissioner's order has a cause of action for damages.[20]

For more information, visit www.oipc.bc.ca

If you have any questions about these guidelines, please contact:

British Columbia
Tel: (250) 387-5629 (in Vancouver call (604) 660-2421; elsewhere in BC call 1-800-663-7867
Email: info@oipc.bc.ca

This guideline was prepared to help organizations and public bodies to comply with the *Personal Information Protection Act* (PIPA) and the *Freedom of Information and Protection of Privacy Act* (FIPPA). This guideline is an administrative tool intended to assist in understanding these Acts. It is not intended to be relied on as legal advice and cannot be relied on as such. For the exact wording and interpretation of PIPA and of FIPPA, please read them in their entirety. This document is not binding on the Information and Privacy Commissioner for British Columbia.

[19] Both the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* provide authority for the Commissioner to conduct an investigation whether the Commissioner receives a complaint or not.
[20] See section 57 of the *Personal Information Protection Act.*