Office of the Information and Privacy Commissioner of Alberta

Guidelines for Social Media Background Checks
December 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 legal and policy implications. Like a credit or criminal background check, many employers, volunteer agencies, and other organizations are now conducting social media background checks on future and prospective employees and volunteers. 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 of Alberta ("OIPC") has developed these guidelines to help organizations navigate social media background checks and privacy laws. The OIPC is concerned that organizations may be implementing social media background checks without fully understanding the legal implications of doing so.

A "social media background check" can mean many things. It can be as simple as checking 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]

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 search for information about an individual, the collection, use, and disclosure of that personal information is subject to the privacy provisions of the *Personal Information*

[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.

Protection Act (PIPA) here in Alberta. PIPA applies to Alberta organizations and fully to some non-profit organizations and on a limited basis to certain non-profit organizations[6].

Putting social media background checks in context

While social media background checks may appear enticing, the reality is that many risks associated with conducting social media background checks exist. As a result, organizations need to clearly understand the legal implications associated with conducting a background check using social media in order to properly assess the risks of using social media for background checking.

There are legal implications that organizations must consider prior to performing social media background checks.

In particular, organizations need to ensure that they comply with the requirements in PIPA with respect to the collection, use and disclosure of personal information and personal employee information, as well as ensure the collection, use and disclosure is reasonable. Organizations also need to recognize that using social media for background checking may result in non-compliance with PIPA because there is no ability to control the amount of information collected, which may result in the collection of irrelevant or too much information about an individual, and collection of third party information. In addition, issues associated with consent and accuracy need to be considered.

Personal information and personal employee information are defined separately in PIPA, and the provisions regarding consent to collect personal information and notice to collect personal employee information should be reviewed carefully by organizations.[7]

Is a social media background check reasonable?

Prior to using social media background checks to collect personal information, an organization must understand its business purpose for doing so, and consider the reasonableness of doing such a check. Under PIPA, an organization must be able to establish that use of social media to collect personal information or personal employee information is reasonable for the purposes of collection. Organizations need to consider what a social media background check will provide that cannot be garnered from traditional means such as reference checks and interviews.

There are other legislative requirements that Organizations should be aware of when collecting personal information via a social media background check such as the *Alberta Human Rights*

[6] Section 56 (b) provides that PIPA does not apply to a "non-profit organization", which is defined in PIPA as "an organization that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*, or that meets the criteria established under the regulations". For these non-profits, PIPA applies only to personal information collected, used or disclosed in connection with a commercial activity. Any non-profit organization not meeting the definition of "non-profit organization" in PIPA is required to comply fully with the requirements in the Act for all personal information collected, used or disclosed.

[7] See sections 1(1)(k) and 1(1)(j) for definitions of personal information and personal employee information, respectively. Sections 15, 18, and 21 establish the conditions under which an employer may collect, use or disclose personal employee information without the consent of the employee. Certain provisions must be met.

Act. It would not be reasonable to collect personal information under PIPA that violates the *Alberta Human Rights Act*.

Are you collecting irrelevant and too much personal information?

The lack of control over the collection of personal information from social media websites creates a risk for organizations of non-compliance with PIPA.

Like a dragnet, social media background checks can catch much more than what was intended. Individuals performing the checks could collect personal information that is irrelevant. Under privacy laws, organizations can only collect personal information that a reasonable person would consider appropriate in the circumstances.

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

Are you collecting third-party personal information?

Of particular importance in social media background checks is the inadvertent collection of third-party personal information. For example, if an organization obtains consent from an employee or volunteer to view his or her profile on Facebook for a reasonable purpose, in viewing that individual's Facebook profile, the organization may be collecting personal information without consent about other individuals who have posted on the Facebook profile page. While organizations can in certain circumstances collect personal employee information without consent, they must take into account that using social media to collect personal information about an employee will likely result in the collection of a third party's personal information, which may constitute a violation of PIPA.[8]

*Of particular importance in social media background checks is the **inadvertent collection of third-party** personal information.*

Even if an organization was in a position to only collect personal information about a single individual on a social media website, the organization may have difficulty meeting the reasonableness requirements if its collection results in the collection of more personal information than is needed to meet the purpose of the collection.

As can be seen, the lack of control over the collection of information from social media websites creates a risk for organizations of non-compliance with PIPA.

[8] See section 7(1)(b) of PIPA.

Are you over-relying on consent?

An organization needs to be aware that obtaining consent to perform a social media background check presents some further challenges that the organization must consider in addition to those challenges noted above.

Under PIPA, organizations can ask an individual for consent to access their social media content; however, PIPA permits the individual to withdraw consent at any time. If an individual withdraws consent to use his or her social media content, the organization cannot not use that personal information to make a decision about the individual.

Obtaining consent to perform a social media background check presents challenges that an organization must consider.

An exception to the ability of an individual to withdraw his or her consent is in the case of an employer who collects the information solely for the purposes of establishing, managing or terminating an employment or volunteer relationship or managing a post-employment or post-volunteer work relationship, and that collection is reasonable. For a current employee notice must be given prior to collection.

Organizations may find it difficult, even with consent, to meet the requirement that collection and use of personal information is reasonable when the information comes from social media sites. For example, even if a job applicant gives an employer permission to access her online dating profile, this collection would likely be found to be unreasonable for the purposes of evaluating the individual's qualifications for the job.

Are you collecting accurate information?

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. An organization might be required to guess which social media account matches the name on a resume, and screen out a potential candidate based on incorrect information. Other factors that can compromise the accuracy of social media include mislabelled photographs and out-of-date information.

Privacy laws require organizations to take steps to ensure that the information they collect is accurate.[9] Viewing is a form of collection under PIPA[10]. An organization that is viewing information that may be inaccurate may find it difficult to meet the requirements in section 33 of PIPA, which requires an organization to "*make a reasonable effort to ensure that any personal information collected, used or disclosed…is accurate and complete*".

Another issue that arises when organizations use social media is that organizations have no way of determining if the information they are collecting is current. Someone might post photographs of someone on a social media site that is several years old. In addition, most

[9] The accuracy requirement applies to any personal information an employer uses to make a decision about that individual. See section 33 of PIPA.

[10] 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). See also OIPC AB Order P2006-008.

social networks make information available indefinitely. Other forms of background checks allow the screener to limit the personal information collected to a specific time period.[11]

What to consider

Organizations must not use social media to perform background checks if doing so results in non-compliance with PIPA. Below is some guidance on what to consider prior to performing a social media background check:[12]

1. Determine what the business purpose is for performing a social media background check. Do you reasonably require personal information that cannot be obtained through traditional means such as interviews or reference checks?
2. Recognize that any information that is collected about an individual is personal information or personal employee information and is subject to privacy laws.
3. Consider the risks of using social media to perform a background check. Conduct a privacy impact assessment to assess the risks. When conducting this assessment, organizations should:
    a. find out what privacy law applies and review it, ensuring that there is authority to collect and use personal information;
    b. determine whether the identified purposes for the collection and use of personal information are authorized;
    c. consider and assess other reasonable measures that achieve the same purpose;
    d. 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 the individual and others that may be inadvertently collected as a result of the social media background check;
    e. identify the risks of non-compliance with PIPA associated with the collection and use of this personal information, including risks associated with the collection of third party personal information and actions taken based on inaccurate information;
    f. 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 using social media;
    g. determine if the collection is authorized and obtain any necessary consents, and for current employees notify the individual that you will be performing a social media background check and tell the individual what you will be checking and what the legal authority is for collecting the personal information; and
    h. be prepared, upon receipt of a request for access, to provide access to the information you collected and used to make a decision about an employee or volunteer.

[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 a friend) might post a photograph years after it was taken. The posting will show up as new when the actual contents of the post could be old.

[12] This guidance is non-exhaustive and provides some (not all) of the things to consider. 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.

What to avoid

1. **Do not wait until after you conduct a social media background check to evaluate compliance with privacy legislation;**
2. **Do not assume in advance that a social media background check will only retrieve information about one individual and not about multiple individuals;**
3. **Do not perform a social media background check from a personal account in an attempt to avoid privacy laws;**
4. **Do not attempt to avoid privacy obligations by contracting a third party to carry out background checks; and**
5. **Do not perform a social media background check thinking that an individual will not find out about it. For example, an individual can use web analytics to determine what IP address accessed the individual's personal information.**

Once collected, personal information can be very difficult to disregard. If an individual suspects that his or her personal information was improperly collected, the individual has a right to complain to the Information and Privacy Commissioner of Alberta (the "Commissioner").[13]

The Role of the Commissioner

The Commissioner has statutory authority to investigate compliance with privacy laws.[14] The Commissioner has the power to require an organization to respond to questions under oath about how they have collected, used or disclosed personal information. If the Commissioner determines that an organization has violated privacy laws, the Commissioner can issue an order compelling the organization to take remedial action. In some circumstances, an individual affected by a Commissioner's order has a cause of action for damages.[15]

[13] 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 they believe that an employer has failed to respond adequately to questions about how the employer has used and disclosed their personal information.
[14] The *Personal Information Protection Act* provides authority for the Commissioner to conduct an investigation whether the Commissioner receives a complaint or not.
[15] See s. 36 of the *Personal information Protection Act*.

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

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

Tel: (780) 422-6860 (toll free 1-888-878-4044)
Email: generalinfo@oipc.ab.ca

This guideline was prepared to help organizations comply with the *Personal Information Protection Act* (PIPA). This guideline is an administrative tool intended to assist in understanding PIPA. 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, please read it in its entirety. This document is not binding on the Information and Privacy Commissioner of Alberta. We would like to thank the Office of the Information and Privacy Commissioner of British Columbia for their collaborative effort in the development of this publication.