Collecting Information via Social Media (Employee and Background Checks)

Social media is a term used to describe on-line technologies, applications and practices used to share information, knowledge and opinions (e.g. social networking sites, blogs, wikis, content sharing sites, photo sharing sites, and video sharing sites). Well-known platforms include Facebook, Twitter, Instagram, YouTube, Reddit, Pinterest and LinkedIn. A social media employee or background check can include a variety of activities ranging from simply checking a Facebook profile to searching all platforms for all information about an individual.

Public bodies may want to obtain personal information from social media in a number of contexts, including:

- vetting employment candidates; or
- monitoring the conduct of current employees.

Collecting personal information via social media is a form of indirect collection. Before any indirect collection of personal information occurs, public bodies must first determine whether the *Act* permits it. This guidance should assist public bodies in making those determinations.

Section 62 (1) of the *Access to Information and Protection of Privacy Act, 2015* ("*ATIPPA, 2015*" or "the *Act*") requires public bodies to collect personal information directly from individuals unless indirect collection is permitted as set out in section 62(1)(a), (b), (c) or (d).

Vetting Employment Candidates

When applying for employment candidates usually provide references. Public bodies can indirectly collect information about the candidate from these references. The candidate implies consent for this collection through the provision of a reference's contact information.

Consent

Generally, candidates do not list or authorize access to their social media platforms. Even if a candidate consented to a social media background check, due to the concerns and issues with the content of social media, as discussed below, public bodies should avoid collecting and using this information.

Public bodies should also be mindful that social media background checks inevitably collect the personal information of other persons who have not consented to any form of collection of their personal information.

Increasingly, judicial and other authorities are recognizing that reasonable expectations of privacy can exist despite individuals sharing personal information in circumstances where they have limited control over who has access to it.[1]

[1] *R. v. Marakah*, SCC 59 (CanLII).

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

Accuracy

The *Act* also requires that public bodies take all reasonable measures to ensure the accuracy of personal information if used to make a decision about a person:

> *63. Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete.*

Information collected via social media can be unreliable and inaccurate. Public bodies can easily link images and information collected from social media to a name, which increases the likelihood that the check will contain inaccurate personal information. Public bodies might guess which social media account matches the name on a resume and screen out a candidate based on incorrect information. In other cases, public bodies might access a social media account set up by an imposter to discredit someone. Other factors can compromise the accuracy of social media, including mislabeled photographs and out-of-date information. Similarly, there is no requirement for individuals to be truthful in the information they post to social media.

Public bodies performing social media background checks could also collect personal information that might be irrelevant and prejudicial. Some information may relate to activities that occurred several years ago regardless of the date posted. Questioning employment candidates about sexual orientation, health status, religion and many other matters are discriminatory and prohibited. Public bodies accessing that type of personal information via social media may have to defend against allegations of discrimination contrary to the *Human Rights Act, 2010*.

Minimum Amount Necessary

Even with an individual's consent, public bodies will have to demonstrate that they used the minimum amount of personal information necessary to accomplish the purpose for which they used it.

Monitoring the Conduct of Current Employees

Public bodies can require that employees adhere to reasonable policies regarding the acceptable use of social media. Public bodies must ensure that employees are aware of their social media policies and the potential consequences for violating those policies.

Public bodies can indirectly collect information via social media to identify potential instances of non-compliance. Public body employees authorize the indirect collection of this information by accepting employment according to its terms and conditions, including social media policies if notified at the time of hire. Arguably, collection of this personal information relates directly to and is necessary for activities of public bodies.

Examples of public body social media policies include:

- Government of Newfoundland and Labrador;
- Social Media Policy - Eastern Health; and
- Social Media Guidelines - Memorial University.

Public bodies checking employee's social media activities must bear in mind all of the above-noted issues regarding reliability, accuracy, relevancy, discrimination and impacts on third parties.

Further, in a recent decision out of Quebec, *Maison St-Patrice inc. et Cusson*, an administrative tribunal refused to allow an employer to rely upon content posted on Facebook that had access limited to an audience controlled by the employee's Facebook privacy settings. The employer obtained the content in question from a friend of the employee with access to it according to the employee's privacy settings.

Conclusion

After confirming their authorization for the indirect collection of personal information via social media and ensuring compliance with applicable privacy legislation, public bodies should not:

- assume that a social media background check will only retrieve information about one individual and not about multiple individuals;
- assume that the account in question was established by the person in question;
- perform a social media background check from a personal account in an attempt to avoid privacy laws;
- attempt to avoid privacy obligations by contracting a third party to carry out background checks; or
- 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.

Individuals who believe on reasonable grounds that their personal information has been collected, used or disclosed contrary to the *Act* can complain to the Commissioner pursuant to section 73. The Commissioner can also commence an own motion investigation into such matters. Individuals also have a right to request access to the information collected and used by a public body to make a decision about a candidate or employee and the public body is under an obligation to keep such records for one year.

This guidance does not apply to information collected via social media for the purposes of law enforcement, defined in section 2(n) of the *Act* as:

> *(n) "law enforcement" means*
> *(i) policing, including criminal intelligence operations, or*
> *(ii) investigations, inspections or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead to or could lead to a penalty or sanction being imposed under the enactment.*