YOUNG ANDERSON
BARRISTERS & SOLICITORS

PROTECTION OF PRIVACY: THE OTHER SIDE OF THE FOI COIN

DECEMBER 2, 2011

Joanna Track

PROTECTION OF PRIVACY: THE OTHER SIDE OF THE FOI COIN

I. INTRODUCTION

The *Freedom of Information and Protection of Privacy Act* came into force in 1992. The purposes of the Act are expressed in section 2 as follows:

> 2 (1) The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by
>
> (a) giving the public a right of access to records,
>
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
>
> (c) specifying limited exceptions to the rights of access,
>
> (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and
>
> (e) providing for an independent review of decisions made under this Act.
>
> (2) This Act does not replace other procedures for access to information or limit in any way access to information that is not personal information and is available to the public.

"Personal information" is broadly defined in Schedule 1 to the Act, and includes any recorded information about an identifiable individual other than business contact information.

The goals of the Act are clearly twofold: accountability through a public right of access to records, and protection of privacy from the unauthorized collection, use and disclosure of personal information. Since 1992, most of the focus for local governments has been on the freedom of information provisions in Part 2 of the Act, and local governments have become quite familiar with receiving and responding to access to information requests. However, less attention has been given to the other aspect of the Act – the regime of personal privacy protections contained in Part 3. While the access to information aspect of the legislation is often seen to have a greater impact on local governments, the privacy protection rules set out within the Act govern the everyday collection, use, disclosure and destruction of recorded information about individuals by local governments. Local governments should be very familiar

with these privacy rules, and should review their practices to ensure they are complying with these requirements at all times.

Part 3 of the Act sets out a comprehensive scheme for the collection, protection, retention, and use of personal information by public bodies, and the purpose of this paper is to highlight the essential elements of this scheme and how they should be applied to local government practices. This paper will also reference a number of decisions of the Office of the Information & Privacy Commissioner (OIPC) as they relate to protection of personal privacy, as well as the recent BC Provincial Court decision *R. v. Skakun*, [2011] B.C.J. No. 1022, in which a municipal councillor was found guilty of breaching section 30.4 of the Act by releasing personal information to the CBC.

II. PURPOSE FOR WHICH PERSONAL INFORMATION MAY BE COLLECTED

Section 26 of the Act provides that personal information may only be collected by or for a public body in certain limited circumstances:

> 26 No personal information may be collected by or for a public body unless
>
> (a) the collection of that information is expressly authorized under an Act,
>
> (b) that information is collected for the purposes of law enforcement, or
>
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

The Act is silent on the burden of proof in relation to section 26, and the OIPC has confirmed that, in the absence of a statutory burden of proof, it is incumbent upon both parties to bring forward evidence in support of their positions. In some cases, where the purposes for which the personal information has been collected may well be unknown to the applicant, the burden will fall heavier on the public body to establish that personal information about an applicant has been collected by it for a purpose described in section 26.

In most circumstances, local governments will be collecting information under subsection (c), where it relates directly to and is necessary for an activity of the local government. For example, information that must be collected in an application for a permit from the local government.

The question of whether personal information is directly related to and necessary for an activity has been considered in a number of decisions from the OIPC. In Order 07-10, the Commissioner considered whether the collection of personal information through an online assessment was

directly related to the Board of Education's recruitment process for new teachers under section 26(c) and whether it was necessary. The complainants argued that the Board had not established a "demonstrable need for the information such that the operating program or activity would not be viable without it", and thus the information collected did not relate directly to and was not necessary for the program or activity, as required under section 26(c). The Commissioner found that, although the *School Act* does authorize the Board to employ those persons the Board considers necessary for the conduct of its operations, the implicit need to collect personal information for the purpose of employing such individuals does not meet the test under section 26(a). However, the Commissioner did conclude that the personal information collected through the online assessment was "necessary" for the Board's operating program or activity of recruitment and hiring, in accordance with section 26(c). The Commissioner stated:

> A relevant part of the interpretive context of s. 26(c) and FIPPA overall is the reality that governments need personal information to do their work. They cannot provide services, confer benefits or regulate conduct without our personal information. For this reason, citizens may be compelled by law to give up their personal information or will disclose it to receive services or benefits and one cannot ignore the power of the state in relation to personal information collection in interpreting what is meant by "necessary" in s. 26(c).
>
> The collection of personal information by state actors covered by FIPPA – including local public bodies such as the Board – will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.
>
> At the same time, I am not prepared to accept, as the Complainants contend, that in all cases personal information should be found to be "necessary" only where it would be impossible to operate a program or carry on an activity without the personal information. There may be cases where personal information is "necessary" even where it is not indispensible in this sense. The assessment of whether personal information is "necessary" will be conducted in a searching and rigorous way. In assessing whether personal information is "necessary", one considers the sensitivity of the personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection. In addition, FIPPA's privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection.

Thus, in determining whether personal information relates directly to and is necessary for an operating program or activity of a local government, and thus is properly collected under section 26(c), the OIPC will consider the nature and extent of the information collected, the sensitivity of the information, and the local government's purpose for the collection. Local governments need not to show that personal information is indispensible to the viability of the project or activity, but must ensure that collection is more than desirable or convenient.

III. HOW PERSONAL INFORMATION IS TO BE COLLECTED

Section 27(1) of the Act provides that a public body can only collect personal information directly from the individual the information is about, except in certain circumstances. The exceptions include where another method of collection is authorized by the individual, the Information and Privacy Commissioner, or by another enactment, or where the information is collected for the purpose of determining suitability for an honour or award, or for the purpose of collecting a debt or fine. This means that a local government must not collect personal information from another public body, or from any other third person, unless to do so falls within one of the listed exceptions to the general rule.

Section 27(2) also requires every public body to tell an individual from whom it collects personal information, the following:

- the purpose for collecting it,
- the legal authority for collecting it, and
- the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

In other words, on every application for a building permit, business licence or in any other circumstance where a local government is collecting personal information, the above details should be written clearly on the form being used by the local government. The requirement in section 27(2) does not apply in certain circumstances, including where the information is about law enforcement or where the minister responsible for the Act excuses a public body from complying with that requirement.

In Order 07-18, the complainant, a former employee of UBC, was terminated from his employment based, in part, on allegations regarding his personal internet use. UBC had utilized log file reports and computer spyware for the purpose of tracking the complainant's internet activity, and the complainant alleged this collection of his personal information was contrary to sections 26 and 27 of the Act. The Commissioner agreed that the collection of the complainant's specific activities was not authorized under section 26 because it was not necessary for the management of the complainant's employment, given that UBC had never raised any concern about the complainant's internet activity with the complainant. In

particular, the collection of screenshots was not necessary to determine the extent of the complainant's non-work related internet usage, and amounted to a particularly severe breach of his privacy rights. The Commissioner also found that it was unreasonable for UBC to initiate surreptitious surveillance of the complainant's behavior when the employer had taken no other steps to address the issue. With respect to section 27, the Commissioner concluded that the manner of collection was contrary to subsection (2), since the requirements for advance notice were not met. UBC argued that it gave the complainant notice of its investigation in the disciplinary meetings which occurred after the information had been collected. The Commissioner rejected this argument, finding that the requirement for notice set out in section 27(2) requires "advance notice".

The OIPC has found that employee surveillance may be acceptable in certain situations, which must be defined and communicated to employees beforehand. However, as the Privacy Commissioner of Canada said in a 2006 news release:

> Workers do not check their privacy rights at the factory or office door. Workplace privacy is an important part of the basic autonomy rights of individuals. Employers must find ways to weed out the bad employees without shattering the dignity and privacy rights of the good employees – who make up the vast majority of the workforce.

In recent years, many public bodies have considered the installation and use of surveillance systems in open public spaces, raising concerns from the OIPC about the impact of such surveillance on the privacy rights of individuals. As discussed, under section 26 of the Act, public bodies may only collect personal information if such collection is authorized by statute, if the information is collected for the purposes of law enforcement, or if the information relates directly to and is necessary for an operating program or activity of the public body. The Act defines "law enforcement" as policing, including criminal intelligence systems, and investigations or proceedings that lead or could lead to a penalty or sanction being imposed. Under section 27, the information must be collected directly from the individual it is about, and the individual must be informed of the purpose for collecting it. A public body must be prepared to demonstrate to the OIPC, with specific evidence, that its proposed or existing collection of personal information by surveillance system is authorized under the Act.

The OIPC has issued a set of Public Surveillance System Privacy Guidelines to assist public bodies in deciding whether collection of personal information by means of a video, audio or other mechanical or electronic surveillance system is both lawful and justifiable as a policy choice and, if so, how privacy protection measures should be built into the system (available on the OIPC website at: http://www.oipc.bc.ca/advice/VID-SURV%282006%29.pdf). The OIPC has made it clear that it is not sufficient to say that citizens need not fear surveillance if they have nothing to hide. Privacy is a fundamental human and civil right that has constitutional dimensions and is recognized and protected by the Act; it should not be easily eroded.

IV. ACCURACY OF PERSONAL INFORMATION

Section 28 of the Act imposes a positive obligation on every public body to make a reasonable effort to ensure all personal information is accurate and complete, where that personal information will be used to make a decision that directly affects the individual:

> 28 If
>
> (a) an individual's personal information is in the custody or under the control of a public body, and
>
> (b) the personal information will be used by or on behalf of the public body to make a decision that directly affects the individual,
>
> the public body must make every reasonable effort to ensure that the personal information is accurate and complete.

In Order 10-31, the complainant consented to the Ministry of Children and Family Development conducting a prior contact check for the benefit of the complainant's new employer. In the process of conducting the check, a Ministry social worker came across a decade-old and uninvestigated allegation of sexual abuse against the complainant. The social worker recommended to the employer that the complainant be barred from unsupervised contact with youth, which resulted in his termination. The complainant argued that the Ministry did not take reasonable steps to assess the accuracy of the information before it used the information in the decision to recommend the complainant be supervised in the workplace.

The Commissioner first considered whether the Ministry "used" the complainant's personal information within the meaning of section 28. The Commissioner concluded that the social worker did employ the information in a manner to accomplish the public body's objectives, and so "used" the information in making her recommendation. The Commissioner then considered whether the personal information was used "in a decision that directly affected" the complainant, within the meaning of section 28. The decision in question was not the decision to fire the complainant, which was made by the complainant's employer, but the decision to recommend the suspension of the complainant's unsupervised contact with youth at his new job. The Commissioner concluded that the information was used in a decision that directly affected the complainant, as the decision to make the recommendation clearly had profound consequences for him. The Commissioner went on to conclude that the Ministry did not make every reasonable effort to ensure the accuracy and completeness of the personal information before using it to make its recommendation, stating:

> What is "reasonable" with respect to s. 28 will be contextual, but the evidence in this case leads me to conclude that the standard

> of reasonability with respect to prior contact checks will generally be higher in the presence of any of the following factors:
>
> - the decision may have a serious impact on the individual's health, safety, finances, employment or reputation;
> - the personal information was not collected directly from the person concerned and the person concerned has not reviewed the information;
> - the personal information is outdated or archived;
> - the personal information is being used for purposes secondary to the original purpose for which it was originally collected;
> - the personal information was supplied anonymously.
>
> The presence of any one of these factors increases both the risk that use of the personal information could have an adverse effect on the person concerned and the obligations on the part of the public body to ensure the accuracy of personal information before it is used in a decision that affects someone.

Thus, the question of whether a public body has made every reasonable effort to ensure that collected personal information is accurate and complete will be contextual, but the standard of reasonability will be affected by the presence of certain factors.

Section 29 allows an applicant who believes there is an error or omission in his or her personal information to request the head of the public body that has the information is its custody and control to correct the information.

Section 31 of the Act also requires that, if personal information is in the custody or under the control of a public body, and is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.

V. PROTECTION OF PERSONAL INFORMATION

Sections 30 and 30.1 of the Act read:

> 30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.
>
> 30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:
>
> > (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
> >
> > (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
> >
> > (c) if it was disclosed under section 33.1 (1) (i.1).

Thus, there is a positive duty on local governments to protect personal information in their custody and under their control, and to ensure that such information is stored only in Canada, unless one of the listed exceptions applies.

In Order 07-10, the complainants contended that, in allowing the online assessment of teaching applicants to be developed and administered in the United States, the Board of Education had contravened sections 30 and 30.1. The complainants argued that the Board had not provided any assurances that the US company administering the assessment and collecting the information was in compliance with the Act's requirements for retention, storage and disposal of personal information. The Board acknowledged that its duty under section 30 to ensure that reasonable security arrangements are in place extends to its service providers, and submitted that it discharged its duty to protect personal information through contractual provisions governing confidentiality. The Commissioner agreed with the Board and made the following statements regarding the duty to protect personal information under section 30:

> The s. 30 requirement to make reasonable security arrangements does not foreclose the possibility of contracting out services involving the collection, use, storage and disclosure of such information. Although public bodies can contract out services, it is well established that they cannot contract out of their privacy obligations under FIPPA. […]

> The mere fact that a public body enters into a contract with a service provider does not contravene s. 30. The public body must, however, ensure that the service provider is contractually required to have standards and policies in place to provide the level of security required under Part 3 of FIPPA. In assessing the "reasonableness" of the security arrangements, consideration must be given to the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure.

In the absence of evidence establishing that the Board had failed to make reasonable security arrangements through its service agreement with the US service provider, the Commissioner concluded there was no basis for finding that the Board had contravened the requirements of section 30.

The complainants also alleged that the Board violated section 30.1 because storage of and access to the personal information of the applicants was in the United States. The Commissioner found that the applicants provided valid consent under 30.1(a) by reading the introductory page of the assessment and clicking the "I consent" button.

The OIPC has issued OIPC Guideline 01-02, Guidelines for Data Services Contracts to assist public bodies in meeting their privacy protection obligations under section 30 of the Act (available on the OIPC website at http://www.oipc.bc.ca/advice/Guidelines-Data_services.pdf). Because the complexity of contractual arrangements varies depending on the nature of the personal information in question and the nature of the services to be provided, it is within a public body's discretion to decide which, if any, of the provisions in the guidelines it will implement from time to time.

VI. UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION

Under section 30.4 of the Act, an employee, officer or director of a public body, or an employee or associate of a service provider who has access to personal information in the custody or control of a public body (whether access is authorized or unauthorized), must not disclose that information except as authorized under the Act. Under section 30.5 an employee, officer or director of a public body, or an employee or associate of a service provider, who knows there has been an unauthorized disclosure of personal information, must immediately notify the head of the public body. Section 74.1 of the Act provides that a person who contravenes section 30.4 or section 30.5 commits an offence and is liable to a fine of up to $2,000.

However, section 30.3 provides protection for employees who disclose personal information in good faith in specific circumstances, and is called the "whistleblower protection":

> 30.3 An employer, whether or not a public body, must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee of the employer, or deny that employee a benefit, because
>
> (a) the employee, acting in good faith and on the basis of reasonable belief, has notified the minister responsible for this Act under section 30.2,
>
> (b) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that the employer or any other person has contravened or is about to contravene this Act,
>
> (c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene this Act,
>
> (d) the employee, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of this Act, or
>
> (e) the employer believes that an employee will do anything described in paragraph (a), (b), (c) or (d).

In what appears to be the first-ever prosecution under the Act, a Prince George councillor (the "Councillor") was charged in 2009 with breaching section 30.4 of the Act by disclosing an *in camera* document containing sensitive personal information, and he attempted to rely on the whistleblower protection under section 30.3 as a defence (*R. v. Skakun*, [2011] B.C.J. No. 1013). The Councillor was elected to hold office in the City of Prince George in 2005. As a result of written complaints made by two City employees, the City's administration retained a third party to conduct a confidential harassment complaint investigation. The investigator sent her report to the City's administration staff in a letter marked "personal and confidential". The administration staff took steps to maintain the confidentiality of the report, because it contained extensive personal information of named individuals. At a closed meeting of Council in April 2008, the Councillor brought a motion that the City administration be directed to provide a descriptive report to Council summarizing the findings of the investigator's report at a subsequent meeting. The report was given to the mayor and City councillors, including the Councillor, for consideration in a closed meeting held in May 2008. At trial, the Councillor testified that, after receiving the report from the City administration for the purposes of the closed council meeting, he personally delivered the report to "someone" at the CBC. The report

was subsequently posted on the CBC's website. The Councillor claimed that the reference to "officer" in section 30.4 of the Act did not include a City councillor, and that the "whistleblower" defence applied to the facts.

The British Columbia Provincial Court convicted the Councillor, finding that nothing in the Act authorized the release of personal information by a councillor acting alone as an officer of the City. The Court found no basis to restrict the meaning of the word "officer" so as to exclude City councillors. City councillors occupying an office are defined as "municipal public officers" under the *Local Government Act* and, as a result, are officers of the public body. The Councillor was an officer of the public body – the City – with access to personal information in the possession of the public body, which he disclosed without authorization as provided in the Act. In doing so, he contravened section 30.4 of the Act.

The Councillor argued that he was a "whistleblower" and therefore could not be found guilty under the Act. In considering whether or not such a defence was available here, the Court stated:

> The whistleblower exception has been defined by the Supreme Court of Canada dealing with cases exclusively in the employer and employee relationship to require the applicant for whistleblower protection to prove the government was acting in an illegal capacity or that health and safety of others was being jeopardized by the conduct of the government. In order to rely upon the defence, an accused is also required to prove that he brought his concerns to the attention of the appropriate authorities and exhausted all of the internal recourses available to him prior to the disclosure of the confidential information.

Both the Crown and the Councillor agreed that the Councillor was not an employee of the City of Prince George. Accordingly, the Court found that:

> If Mr. Skakun was not employee, then he is not a whistleblower recognized in the existing civil case law. The case law has provided the benefit of whistleblower status to employees. That distinction is reflected in s. 30.3 of the Act.

Even if the Councillor could be considered an employee for the purposes of the whistleblower protection, the Councillor still had to show that his actions fell within the limited exceptions to the general duty of loyalty. The Councillor argued that he had a right to disclose the document due to the "government illegality" exception. He turned to the Supreme Court of Canada's decision in *Fraser v. Public Services Staff Relations Board*, [1985] 2 S.C.R. 455, in which the Court found that employees under a duty of loyalty or another oath of secrecy or confidentiality are entitled to break the duty or oath if they seek to expose an illegal act or if policies jeopardize the life, health or safety of others.

The Court in *R v. Skakun* concluded that it was not open to the Councillor to suggest he had the right to disclose the document due to the "government illegality" exception. The Councillor did not testify about any illegal act or immediate jeopardy to the life, health or safety of others, and so no such exception could provide a basis for the disclosure of the report. Further, the Councillor did not exhaust internal resources before making the report public. The Court found that the Councillor had an opportunity to place a motion before Council asking that the report be disclosed in accordance with the Act, but he did not do so. He did not take a single step to use any internal process to disclose the information he wished to disclose. He took it upon himself to disclose the report to the media and, by doing so, he ignored the safeguards and protection afforded by the Act.

The Councillor was found guilty and ordered to pay a fine of $2,000, the maximum fine available under the Act. He has appealed this decision.

It should be noted that council members (including former council members) also have a duty to respect confidentiality under section 117 of the *Community Charter*, and to keep in confidence any record held in confidence by the municipality and any information considered in a closed council meeting. If a councillor breaches section 117 and the local government suffers damage as a result of that breach, the local government can sue the councillor for its damages.

VII. USE OF PERSONAL INFORMATION

Section 32 of the Act provides that, unless the individual consents to an alternative use, a public body may only use personal information for the purpose for which it was obtained or compiled, or for a consistent use:

> 32 A public body must ensure that personal information in its custody or under its control is used only
>
> (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),
>
> (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or
>
> (c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

Section 34 sets out the definition for what is considered a consistent use and specifies that all the information must have a reasonable and direct connection to the purpose for its collection:

> 34 (1) A use of personal information is consistent under section 32 or 33.2 with the purposes for which the information was obtained or compiled if the use
>
> (a) has a reasonable and direct connection to that purpose, and
>
> (b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information or causes the information to be used or disclosed.

In Order 07-10, the complainants argued that the Board of Education's use of personal information collected through the online assessment also violated section 32. The complainants alleged that applicants were notified that the personal information would be used for the hiring and recruitment process, but the information was also used for a number of other purposes that were not disclosed, such as to assess the applicant's teaching and psychological suitability, to provide the applicant with a score percentile, and to screen out applicants at the School District's offices. The Commissioner concluded that section 32(a) authorized the Board's use of the information for its hiring and screening process, and the evidence established that the personal information was being used by the Board for the purpose for which it was obtained and compiled, namely to assist with screening applicants and identifying those who should be short-listed for interviews. Every use by the Board was consistent with that purpose.

It is important to remember that a local government can only use personal information for the purpose for which it was obtained or compiled, or for a consistent use. For example, a local government cannot use personal information obtained as part of a building permit application for the purpose of validating its voter list, as such a use is not consistent with the purpose for which the information was originally obtained.

VIII. DISCLOSURE OF PERSONAL INFORMATION

Section 32 of the Act addresses the use of personal information by the public body, but does not authorize disclosure of the personal information. Disclosure of personal information by public bodies is dealt with in section 33, which says that a public body must ensure that personal information in its custody or under its control is disclosed only as permitted under section 33.1 or 33.2. Together with section 32, these sections give further protection to individuals that their information will not be used or disclosed for unanticipated or inappropriate purposes.

Section 33.1 deals with disclosure inside or outside of Canada, and section 33.2 deals with disclosure inside Canada only. Both sections should be reviewed carefully by local governments

to protect against inappropriate disclosure, including disclosure of information to other local governments. Some examples of when personal information may be disclosed under section 33.1 include: in response to a proper request for access to information in accordance with Part 2 of the Act, where the individual has consented to the disclosure, for the purpose of verifying motor vehicle insurance or drivers licences, and where there are compelling circumstances that affect anyone's health or safety. Some examples of when personal information may be disclosed under section 33.2 include: where necessary to comply with a court order, to the auditor general or any other prescribed person or body for audit purposes, and for law enforcement purposes. A public body may also disclose personal information inside Canada to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister.

NOTES

NOTES