YOUNG ANDERSON
BARRISTERS & SOLICITORS

FOI AND PRIVACY UPDATE

NOVEMBER 27, 2015

David Loukidelis, Q.C., and Maria Kim

FOI AND PRIVACY UPDATE

I. INTRODUCTION

Access to information and privacy cases are making headlines in British Columbia. This year, from investigations into the use of employee monitoring software to the "triple deleting" of government emails, the Office of the Information and Privacy Commissioner for BC ("OIPC") has uncovered major deficiencies in public bodies' compliance with the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). This paper examines a roundup of notable investigation reports and guidelines published by the OIPC on access and privacy, and presents a short freedom of information case law update.

As the independent agency mandated to oversee the information and privacy practices of public bodies, the OIPC launched its audit and compliance program in 2014 to assess the extent of public sector organizations' compliance with FIPPA. Under this program, the OIPC has thus far examined the BC government's privacy breach management (January 2015) and examined selected BC health authorities' privacy breach management (September 2015). It was recently announced that the OIPC will be reviewing access to information practices of the City of Vancouver as its next focus. Accordingly, now, more than ever, there is a need for local governments to undertake a review of both their access to information and their privacy management practices and to implement a comprehensive management framework in line with FIPPA.

II. ACCESS TO INFORMATION

A. Duty to Assist Applicant in Access Request (FIPPA, s. 6)

In a recent investigation report, F15-03, the OIPC examined public bodies' records management and disposal practices, focusing on s. 6(1) of FIPPA (duty to assist applicants):

> The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

This section imposes a duty upon public bodies to make every reasonable effort to assist applicants in access to information requests. The OIPC investigated the practices of three government ministries to determine whether this obligation had been met.

The Commissioner found that certain practices the investigations uncovered were in serious contravention of s. 6(1) of FIPPA. These practices included "triple deleting" emails, permanently deleting emails, overly narrow interpretation of access requests, destruction of non-transitory government records, and negligent searches for records.

First, the OIPC examined aspects of an access request made to the Ministry of Transportation and Infrastructure ("MOTI") concerning missing women along Highway 16 (the Highway of Tears). In particular, records about certain meetings held by MOTI were at issue. MOTI initially identified 36 pages of records as responsive to the request, but upon review of the records, with an overly narrowed interpretation of the request, decided that it had no responsive records. The investigation was prompted by an allegation that a certain employee at MOTI wilfully deleted responsive email records that were potentially responsive to the request by "triple deleting" them. After multiple interviews under oath, and review of available forensic evidence, the OIPC concluded that it was more likely than not that certain responsive emails were intentionally destroyed. The OIPC referred the case to the RCMP for investigation, including the employee's failure to tell the truth under oath.

The second investigation focused on an access request made to the Ministry of Advanced Education for emails exchanged between the Minister's Chief of Staff and the Minister for a specified time period. While the Minister produced a large number of records in the processing of this request, the Chief of Staff did not produce any responsive records. Upon examination of the Chief of Staff's email account, the OIPC found that he had approximately 20 responsive emails that he did not produce. The OIPC concluded that there was a negligent search for responsive records, and thus that the Ministry had contravened its duty under s. 6(1) of FIPPA.

The last investigation concerned the Executive Branch of the Office of the Premier's process for tracking access requests and staff's records management practices. The FOI Coordinator for the Executive Branch stated that once he receives notice of an access request, he personally meets and speaks with each individual within the Executive Branch to ask whether or not they have responsive records. He does not correspond by email or by telephone. His practice is to simply record on a sticky note the people he had talked about the request and destroy the note after dealing with the request.

The OIPC found that personally asking individuals whether they have responsive records, rather than sending an email or otherwise documenting the response process, resulted in no lasting record of the response process. It also creates the potential for systemic delay in access requests in reaching relevant employees and, in some cases, the risk that employees inadvertently delete responsive records, not knowing the request had been received. In addition, the OIPC expressed concerns over the Deputy Chief of Staff's practice of deleting emails from her sent folder on a daily basis, and her belief that very few of the emails she sends are non-transitory.

The Commissioner stated that, under s. 6(1) of FIPPA, an employee's "deleted items" folder must be searched as part of any access request because emails in this folder are readily retrievable by performing an automated search. Where there is a reasonable belief that there are responsive documents in that file, it may also be necessary to perform a search of the "recover deleted items" folder where emails from the "deleted items" folder are moved to.

The public bodies' obligation to search deleted emails that exist only in a backup drive will depend on the situation: under ordinary circumstances, the duty to assist will not require such a search, as it is too costly and time-consuming to be considered reasonable.

In light of the above findings, the Commissioner stressed the need for public bodies to provide mandatory records management training to all employees. The Commissioner also recommended that public bodies configure settings in their email servers to prevent employees from permanently deleting government emails and to ensure all records are backed up. The Commissioner made a number of recommendations that have more general application:

- *Review access to information processes to ensure that requests for records are communicated by email in a timely manner and properly documented.* A system should be put in place that results in access requests being emailed to all employees with potentially responsive records as soon as possible, and to keep reliable electronic records of the responses of individual employees.

- *Clarify access requests with applicants where it is necessary to ensure that the requests are not interpreted too narrowly and to maximize the likelihood of producing records that are responsive to the applicant's request*. The duty to assist an applicant under s. 6(1) of FIPPA requires such clarification where appropriate.

- *Develop a clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access request through access to information training.* Searching for records on a phone, a tablet, or similar device is not a reasonable means of conducting a search; a reasonable search is one that is performed from a desktop or a laptop.

- *Provide mandatory records management training to all employees, that includes the identification of transitory and non-transitory records and the process for retaining and destroying records.* It is a record's content and context that determines whether a record is transitory, rather than its form. Transitory records include convenience copies, unnecessary duplicates and working materials and drafts once the finished record has been produced. Non-transitory records include decision records, instructions and advice (showing how decisions were reached), as well as documentation of a policy matter or how a case was managed. Local governments should ensure they have a good definition of "transitory record" and ensure it is properly applied.

- *Configure settings in email servers to prevent employees from permanently deleting emails and to ensure all government emails are captured in monthly backups.*

The recommendations specifically relating to the Commissioner's interpretation of s. 6(1) of FIPPA (recommendations 1 & 2 above) are now essentially incorporated into public bodies' duties under FIPPA. While the others are recommendations, without necessarily the force of law, local government practices that significantly deviate from these recommendations are likely to attract criticism or concern from the OIPC.

B. Mandatory Disclosure of Records in the Public Interest (FIPPA, s. 25)

In August 2014, the Mount Polley mine tailings pond in the Cariboo Regional District breached, releasing millions of cubic metres of toxic water and mining waste into the nearby lakes. It has been called one of the biggest environmental disasters in modern Canadian history. In response to this disaster, the OIPC conducted an investigation into whether the provincial government had information in its possession about the risk posed by the dam that it should have released to the public prior to the failure. Although the OIPC found that the government did not have information that the dam presented a risk, the Commissioner re-interpreted s. 25(1)(b) of FIPPA to no longer require an element of temporal urgency for the disclosure of information that is clearly in the public interest.

Section 25(1) of FIPPA directs that certain information must be disclosed if it is in the public interest:

> Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information
>
> > (a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or
> >
> > (b) the disclosure of which is, for any other reason, clearly in the public interest.

For twenty years, the OIPC had interpreted this section, and the phrase "without delay," to require an element of temporal urgency to the risk of harm or to the public interest in order to trigger an obligation to disclose information. In other words, there had to be both an urgent or compelling need for the disclosure as well as a clear public interest.

The Commissioner has now revisited this section and found that it is possible to assess whether disclosure of information is in the public interest without necessarily accounting for, or requiring, an element of temporal urgency. She clarified that the requirement for disclosure "without delay" relates only to the timing of the disclosure duty itself. As for what is captured under the term "public interest", the Commissioner provided a few examples, such as those involving the interest of the public in relation to matters of public finance or financial management, or relating to proper public administration. The Commissioner explained that this new interpretation accords with the plain meaning of the language used and is consistent with FIPPA's statutory purpose of making public bodies more accountable to the public.

In light of the revised interpretation, the Commissioner recommended that all public bodies promptly evaluate whether they currently have information that must be disclosed pursuant to s. 25(1)(b), where "a disinterested and reasonable observer, knowing what the information is and knowing all of the circumstances, would conclude that disclosure is plainly and obviously in the public interest." All public bodies are also encouraged to develop policies that provide guidance to employees and officers about the public body's obligations under s. 25 of FIPPA, including specific steps an employee should take to bring relevant information to the attention of the head of the public body. It is important to note that this s. 25 disclosure duty applies despite any other provisions, including the access exceptions found in Part 2 of FIPPA.

The challenge is that it is difficult to provide more specific guidance as to what the "public interest" means, and when s. 25 requires disclosure. Again, the Commissioner referred to disclosure being required where it is "plain and obvious" to a reasonable observer that disclosure is, in the circumstances, in the public interest. One approach would be for local governments to assess their information holdings by subject matter, to identify areas where disclosure might be required.

For example, information about wastewater treatment, or water quality, might, because of the possible public health ramifications, be more likely to have a public interest dimension. Information about other public health issues, including food safety in restaurants, might also be identified as a category amenable to public interest disclosure. A final category of information that could have public interest disclosure implications is in the area of geo-technical information about site or slope stability, or flood plain-related information.

Some local governments have already acted in such areas, by pro-actively disclosing, through websites and other means, information with public health implications or implications for the safety of persons or property.

III. PROTECTION OF PRIVACY

A. District of Saanich's Use of Employee Monitoring Software

Earlier this year, the OIPC released an investigation report, F15-01, finding that the District of Saanich violated employees' privacy rights by installing employee monitoring software on a number of municipal computer workstations. The software, known as "Spector 360", was installed on workstations used by employees and officers of the District whom the District viewed to be "high-profile" and therefore likely targets for an IT security breach. These employees included the Mayor, Councillors, the CAO and the heads of various departments.

The software had a number of what the Commissioner considered to be intrusive features, such as automated screenshots at 30-second intervals; a log of every keystroke made by a user; retention of every email message sent or received; and tracking of every file created, deleted, renamed, or copied. As a result, the software collected all personal information that a user

entered into their workstation, including images of personal Internet use, Internet banking, private passwords, or medical laboratory results, as well as the personal information of any constituents who contacted the high-profile employees.

When questioned by the OIPC about the purpose behind the installation of the software, the District produced its software use policy, which was "to ensure the security and integrity of computers for high profile individuals and protect District information from unauthorized access, theft and destruction." The District emphasized that access to the software and server was restricted to the Manager and Assistant Manager of IT and could only occur as a result of a "security event", such as hacking, data theft, or lost or stolen technology equipment. However, the District was not able to produce any evidence that the information collected was not improperly accessed, as it did not keep an access log.

The OIPC found that the collection of personal information of employees and elected officials through the use of the software was not authorized by FIPPA. While the District had the authority to collect personal information that is directly related to and necessary for the protection of IT systems and infrastructure, tracking every keystroke and email and capturing screenshots of computer activities at 30-second intervals clearly exceeded that purpose. Not only was the District collecting large amounts of personal information, it was found that some portion of that information was sensitive. It went to the "biographical core" of its employees protected by s. 8 of the *Canadian Charter of Rights and Freedoms*, which offers protection against unreasonable search and seizure. The OIPC also found that the District failed to provide adequate notice to employees and elected officials about the amount and type of personal information it was collecting.

The Commissioner made a number of recommendations for change, including disabling all intrusive monitoring functions of the software and destroying all personal information already collected. The Commissioner recommended that the District appoint a chief privacy officer and implement a comprehensive privacy management program, including by updating its privacy policy and staff training. The Commissioner also emphasized that governments should remember, and respect the idea, that employees have an expectation of privacy in the workplace.

B. Pro-active Privacy Management: Best Practices

Local governments collect personal information in order to administer many of their programs, sometimes by compelling citizens to give up their personal information in ways that ordinary businesses cannot. Local governments, therefore, have a legal and moral obligation to responsibly manage personal information in their custody or control. An essential part of building and maintaining public confidence is safeguarding personal information and responding appropriately whenever personal information has been compromised. In light of the Commissioner's recommendations in the Saanich investigation report discussed above, it is

imperative for local governments to consider how their current privacy management program measures up to their privacy obligations under the law, and to train staff in relation to all requirements under FIPPA.

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Privacy breaches can be unintentional or deliberate and may range from unauthorized access to databases of personal information by employees, to inappropriate or accidental disclosure of personal information. Misdirected communication, administrative error, lost or stolen records (or mobile devices holding records), network attacks (e.g., hacking, phishing, malware) are all common examples of how privacy breaches occur.

1. Accountability and Duty to Protect Personal Information

The OIPC views accountability in relation to privacy as accepting responsibility for personal information protection. In order to demonstrate accountability for privacy, the OIPC requires public bodies to have a privacy management program, which includes having comprehensive policies, procedures and practices in place that comply with applicable privacy laws. Local governments must be prepared to provide evidence of privacy management to the OIPC in the wake of an investigation, audit or privacy breach.

Local governments have a legislated duty to protect personal information in their custody or control under s. 30 of FIPPA. This responsibility includes "making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal." Managing privacy breaches forms part of this duty to protect personal information. Section 30 makes it clear why there is a need for local governments to develop and implement a privacy management program and to train employees in their obligations under FIPPA.

2. Privacy Policies and Culture of Privacy Awareness

The first step in implementing a successful privacy management program is developing a strong internal governance structure that focuses on privacy compliance, and to create and maintain a culture of privacy awareness. The executive management of a local government body should ensure that all resources necessary to develop, implement, monitor and adapt the program are available to the privacy officer. While it may be challenging for local governments with scarce resources to develop such a program, it must be remembered that compliance with FIPPA is not optional; the OIPC will expect adequate funding and support to be devoted to privacy compliance.

It is crucial for local governments to develop the following policies addressing these key privacy issues to ensure they are in compliance with FIPPA and in order to be able to demonstrate compliance to the OIPC and to the public:

- Authority for collection, use and disclosure of personal information;
- Requirements for notification prior to collecting personal information;
- Ensuring accuracy of personal information;
- Individual access to and correction of personal information;
- Retention and disposal of personal information;
- Responsible use of information and information technology to protect personal information;
- A process for handling privacy-related complaints; and
- Procedures for managing privacy breaches (containing, mitigation and reporting a breach).

3. Compliance and Monitoring

Once privacy policies are adopted, an internal audit (review) program should be established to evaluate and report on compliance. The OIPC expects public bodies to conduct internal audits of security safeguards as a key component in a privacy management program. The OIPC recommends that internal audit processes include employee interviews and periodic file reviews. External audits by a qualified third party may be warranted when the public body has suffered a significant privacy breach. These audit and compliance reports may help establish due diligence in response to an investigation or audit by the OIPC.

A privacy management program must also clearly define when and how a matter is to be escalated, and to whom. Section 30.5(2) of FIPPA requires that privacy breaches be immediately reported to the head of the public body:

> An employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the head of the public body.

Informing employees of what is required of them in order to protect personal information and in the event of a breach is a crucial part of privacy breach management. In instances of other privacy complaints, progress reports about the handling of a matter should also be reported to the privacy officer. This is necessary to ensure that procedures are being followed and required steps are being taken.

4. Personal Information Inventory and Privacy Impact Assessment

As part of the privacy management program, local governments should also consider establishing a personal information inventory. A thorough inventory will: assist the local government in managing personal information in its custody or control; identify and confirm the authority for the collection, use and disclosure of the personal information; and help assess the sensitivity of personal information. The OIPC suggests that every aspect of a sound and effective privacy management program begins with this inventory, as it is difficult to see how a public body can meet its statutory requirements unless it knows what personal information it collects, how it uses it, to whom it is disclosed, for what purposes, and so on.

A Privacy Impact Assessment (PIA) should be completed for all new projects contemplated by local governments involving personal information and for any new collection, use, or disclosure of personal information. To ensure that the PIAs are conducted, local governments should develop procedures for completing PIAs, involving the privacy officer and staff from all affected operational areas.

5. Employee and Service Provider Training

The OIPC emphasizes the need for regular, mandatory privacy training for all employees regarding the importance of protecting personal information and breach reporting and management processes. Employee training is the key because in order for a privacy management program to be effective, employees must understand and be actively engaged in privacy protection. An effective privacy management program will enable all employees and officials to be aware of, and be ready to act upon, the public body's privacy obligations. The content of the training program should be periodically revisited and updated to reflect changes within the public body, to FIPPA and to industry best practices.

Finally, it must be remembered that any time personal information is disclosed or used by a service provider to the local government, responsibility for privacy compliance remains with the local government. For example, there is a requirement under FIPPA that prohibits public bodies, subject to certain exceptions, from disclosing personal information outside Canada or allowing access from outside Canada. Since cloud services are often utilized in the storage of personal information, local governments should make careful inquiries before entering into service arrangements involving personal information. A privacy management program should, therefore, include procedures for ensuring compliance by contractors with relevant FIPPA obligations and with their contractual obligations to the public body.

6. Privacy Officer's Role

The OIPC suggests that the privacy officers for the public bodies should regularly review their privacy programs to:

- Ensure the public body's personal information inventory is updated, and that new collections, uses and disclosures of personal information are identified and evaluated;
- Revise policies as needed following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices or as a result of environmental scans;
- Treat privacy impact assessments and security threat and risk assessments as evergreen documents, so that changes in privacy and security risks are always identified and addressed;
- Review and modify training on a periodic basis as a result of ongoing assessments, and communicate changes made to program controls;
- Review and adapt breach and incident management response protocols to implement best practices or recommendations and lessons learned from post-incident reviews;
- Review and, where necessary, fine-tune requirements in contracts with service providers; and
- Update and clarify external communications.

IV. FOI CASE LAW UPDATE

Over the last year, the OIPC has affirmed established principles in areas of key interest to local governments. The first decision of interest is Order F15-56, which dealt with an *in camera* report to council relating to a building developer's withdrawal from a partnership with a local government. The OIPC held that the entirety of the report could be withheld because the evidence established that, in this case, disclosure of the report to council would disclose the substance of council's deliberations under s. 12(3)(b) of FIPPA. Earlier OIPC decisions have not gone this way, showing that the facts matter, as does how a local government argues its case.

In Order F15-54, the OIPC held that a university could withhold the entirety of a report into workplace harassment allegations against an employee. The report contained the employee's responses to the allegations, as well as evidence, statements, findings and investigation conclusions. Consistent with previous decisions, the OIPC held that disclosure of this personal

information was presumed to be an unreasonable invasion of the employee's privacy. None of the factors in s. 22(2) rebutted this presumption. The adjudicator found that none of the information could be disclosed without revealing the employee's other personal information, so severing was not required and the entire report had to be withheld.

This decision underscores the need for local governments to have policies around workplace investigations. If confidentiality is desired, this needs to be stated up front, with participants and witnesses being told that their statements and submissions are received in confidence. This does not guarantee that s. 22 will protect the information, or the entire report or file, but assurances of confidentiality can help support application of s. 22 (if that is what the local government wants, as is usually the case). In addition, if a local government is hiring an outside investigator, it should consider who will have custody or control of working papers. Even the OIPC may find that if the local government does, this should be clarified, at the outset, in the service agreement with the investigator.

Consistent with long-standing principles, the OIPC has affirmed over the last year that contracts between public bodies and service providers or other contractors almost always have to be disclosed in their entirety. In Order F15-53, for example, the OIPC held that a food services agreement for a provincial correctional centre had to be disclosed entirely. The pricing in the contract was commercial and financial information, as required by s. 21, but it was found that the agreement terms, including pricing, had been negotiated and not "supplied" to the public body, as required by s. 21.

This decision again illustrates the need for local government procurement processes to address access to information at the start of the process. Potential bidders or proponents should be told, in the RFP or tender invitation, disclosure under FIPPA is a possibility. A local government may accept submissions in confidence, and keep contract negotiations confidential, but no promises should be made, in writing or verbally, that the agreement or contract documents will never be disclosed just because of confidentiality. The situation can differ for tenders or proposals, but draft or final agreements themselves are very likely to have to be released and this should be disclosed at the outset. The procurement documents should also disclaim any liability for the local government if it is required to disclose information in response to an access request. In any case, a local government that receives an access request in such cases—disappointed bidders will often make them, for example—it should nonetheless seek legal advice before disclosing any information.

Finally, the issue of severing "outside of scope" materials from responsive records in Order F14-27 was reconsidered in Order F15-23, where it was decided that a public body is not authorized under FIPPA to sever and withhold portions of responsive records on the basis that they are outside the scope of the applicant's request. This decision and the earlier decisions, F14-31 and F14-32, require local governments to continue to disclose the non-responsive contents of records responsive to access requests unless the severing of the non-responsive contents can be specifically justified under Part 2 of FIPPA.

V. CONCLUSION

As this paper illustrates, this has been an active year for the Commissioner and her Office and it is clear that her energetic, wide-ranging and pro-active approach to compliance audit and investigation will continue. It is, again, important for local governments and all public bodies, to assess how they manage their legislated access and privacy obligations and take steps to ensure, pro-actively and before the Commissioner comes calling, that these duties are managed systemically in an appropriate fashion.

NOTES

NOTES