YOUNG ANDERSON
BARRISTERS & SOLICITORS

PRIVACY AND FOI UPDATE

NOVEMBER 22, 2019

David Loukidelis, QC and Ethan Plato

PRIVACY AND FOI UPDATE

I. INTRODUCTION

Quite a lot of water has gone under the bridge since our last update on privacy and freedom of information. Our goal here is to highlight key trends while pointing you to significant Office of the Information and Privacy Commissioner (OIPC) and court decisions since our last update.

We are confident that you are familiar with the *Freedom of Information and Protection of Privacy Act* (FIPPA), with both its freedom of information and privacy rules. Its goals are stated in the law: to make public bodies – including local governments – more accountable to the public, while also protecting privacy.

FIPPA gives the public, anyone who makes a request to a public body, a right of access to records in custody or control of a local government. FIPPA contains several exemptions to this default right of access. We discuss recent cases about some of these, such as solicitor-client privilege.

FIPPA also has rules governing the collection, use and disclosure of individuals' personal information by local governments and other public bodies. We discuss recent developments in this area as well, including recent amendments related to disclosure of personal information outside Canada.

Our overall message is that freedom of information and privacy are fast-moving, ever-changing, topics, globally and at home and our goal here is to offer a snapshot of selected recent developments for local governments in British Columbia.

II. PRIVACY TODAY

A. Relaxation of Restrictions on Personal Information Storage and Access Outside Canada

In 2004, FIPPA was amended to severely restrict the ability of public bodies to permit the storage of, or access to, personal information from outside Canada (section 30.1).[1] The violation of this prohibition can result in significant fines, including for service providers to public bodies.

[1] The amendments also include strict obligations to report foreign demands for disclosure and unauthorized disclosures of personal information, as well as whistle-blower protections. Again, the amendments also include significant fines for violation of the in-Canada and related requirements.

There are several exceptions to the prohibition, but in practice these have proved to be somewhat limited.[2] The prohibition has presented significant challenges for public bodies seeking to take advantage of modern information technologies, including cloud-based storage and computing services.

These challenges range from the inability of service providers to maintain or repair medical imaging equipment operated by health authorities to, more recently, adoption of cloud-based services such as Microsoft Office 365. The first of these was mitigated by amendments several years ago that permit time-limited remote access to electronic systems or equipment where the access is necessary for the purpose of installing, implementing, maintaining, repairing, troubleshooting or upgrading the system or equipment (section 33.1(1)(p)).[3]

Several efforts have been made over the years to eliminate the in-Canada requirement or expand the exceptions, but these have failed until very recently. On October 31, 2019, amendments to FIPPA came into force that, as we understand it, are intended to enable local governments and other public bodies to take advantage of cloud-based services, including services such as Microsoft Office 365.[4]

Section 33.1(1) has been amended in order to clarify section 33.1(1)(p), which permits temporary access as described above. The more significant changes are the new sections 33.1(1)(p.1) and (p.2).

Section 33.1(1)(p.1) is a detailed provision that now permits disclosure of personal information outside Canada where that is necessary for the processing of information *and* the processing does not involve intentional access to personal information by any individual or result in the storage of personal information (other than personal information that is metadata)[5] outside Canada. In addition, the disclosure outside Canada must be limited to temporary access limited to the minimum time necessary to complete the processing.

[2] The exceptions include cases in which the individuals whose personal information will be stored or accessed outside Canada have identified the personal information and consented, in accordance with the *Freedom of Information and Protection of Privacy Regulation*, to that storage or access. In addition, section 33.1 contains several grounds of authority for disclosing personal information outside Canada and these admittedly do provide some leeway for local governments in the ordinary course of their operations.

[3] The amendments also allow time-limited remote access that is necessary for data recovery following failure of an electronic system.

[4] The amendments were enacted by the *Miscellaneous Statutes Amendment Act (No. 2), 2019*, S.B.C. 2019, c. 36.

[5] The term “metadata” is not defined.

The new section 33.1(1)(p.2) is equally detailed. It permits the disclosure of metadata outside Canada if the metadata is generated by an electronic system and describes an individual's interaction with that system. In addition, personal information in individually identifiable form must, if practicable, have been removed from the metadata or destroyed and, in the case of disclosure to a service provider, the public body must have prohibited any subsequent use or disclosure of personal information in individually identifiable form without the public body's express authorization.

These obviously highly technical amendments are, again, apparently intended to enable adoption by public bodies of services such as Microsoft Office 365. As should be clear from the above description, the amendments do not permit storage of personal information, or access to it, outside Canada. They aim only to permit limited processing outside Canada of information that may include personal information, in the ordinary course of operation of a service.

Any local government considering moving forward with cloud-based services should conduct a privacy impact assessment, consulting with its technical advisors and the prospective service provider, to ensure that the service will comply with the amendments.[6] The service agreement should require the service provider to store personal information, and permit access to it, only inside Canada, the only exception being in accordance with the amendments described here or as otherwise expressly provided in the service agreement.[7] The agreement should require the service provider to comply with FIPPA and, ideally, would specifically require the service provider to comply with the foreign demand notification requirements described above, as well as the full range of FIPPA's in-Canada provisions.[8]

[6] Although it is not mandatory, public bodies sometimes provide draft privacy impact assessments to the OIPC for comment. Although the OIPC will not, for legal reasons, formally approve a privacy impact assessment, its comments can be useful in identifying compliance concerns. We are aware that the provincial government is considering moving forward with cloud-based services and, ideally, it will provide guidance for public bodies on the amendments. We can also hope that the OIPC will provide guidance.

[7] For this reason, it has been reported that Microsoft Canada, to give only one example, has established server facilities in Canada, so that personal information is stored in Canada.

[8] We recognize that, in the case of multinational service providers, it may be difficult to negotiate such terms, but at the very least the service agreement should require the service provider to comply with all applicable laws, including FIPPA. Depending on the nature of the proposed service, the service agreement may well need to include other privacy protection provisions. The provincial government's standard-form general services agreement, which is available online, contains a privacy protection schedule that provides a useful starting point for service agreement privacy provisions. We should always consult legal counsel, of course, before initiating a procurement process for such services, as well as throughout the contract negotiation process.

B. Smart Cities

The concept of a "Smart City" has gained traction in recent years, and has generated a spirited debate pitting privacy rights against technological solutions for local governments. The following definition adapted from Professor Rob Kitchin at Maynooth University in Ireland was recently used in a report on Privacy and Smart Cities by McMaster University:

> A 'smart city' adopts digital and data-driven technologies in the planning, management and delivery of municipal services. Information and communications technologies (ICTs), data analytics, and the internet of things (IoT) are some of the main components of these technologies, joined by web design, online marketing campaigns and digital services. Such technologies can include smart utility and transportation infrastructure, smart cards, smart transit, camera and sensor networks, or data collection by businesses to provide customized advertisements or other services. Smart-city technologies monitor, manage and regulate city flows and processes, often in real-time.[9]

The challenge for all local governments in the coming years will be to appropriately balance the privacy interests of citizens while still leveraging the benefits of a connected city. To illustrate, take the example of data collected from a transit system. A commuter benefits by knowing when their next bus is coming and how crowded that bus is, and a transit authority benefits by knowing which routes are over or under utilized. If that same information is used to push advertisements to commuters for a new car at the times when a transit system is most busy, or be used to influence individual's commuting behaviour, or to adjust prices for alternative transportation methods such as ride sharing or car share programs, then individuals may feel their privacy is violated simply by participating in urban life.

Local governments have the legitimacy and power to be able to collect citizens' data for public purposes. To develop and implement many of these new and innovative services, some form of partnership with the private sector will be necessary and likely inevitable. Exactly what form that balance will take is in the process of being determined across Canada and around the world, with the most high-profile case being the Waterfront Toronto project at Quayside being proposed by Sidewalk Labs, the urban innovation organization of Google's parent company, Alphabet Inc. The proposed development is a pilot "smart" city in a limited area of Toronto showcasing the potential for a completely integrated and connected urban space. Concerns have been raised regarding the sharing of information collected through the project, both with Sidewalk Labs and with other third-party developers plugging into the proposed database. At the time of writing, the Canadian Civil Liberties Association is in active litigation with Waterfront Toronto and the overall project is facing considerable public scrutiny.

[9] Sara Bannerman & Angela Orasch, "Privacy and Smart Cities: A Canadian Survey", online: January 2019 (McMaster University) <https://smartcityprivacy.ca/wp-content/uploads/2019/01/Bannerman-Orasch-Privacy-and-Smart-Cities-A-Canadian-Survey-v1-2019.pdf > accessed November 12, 2019.

Not every iteration of a smart city will take the form of a completely new and distinct neighbourhood, and much of the change for local governments will be incremental and project specific. And while innovative solutions are developed, tested, and implemented, the most prudent course of action a local government can do is to conduct a PIA of any proposed project involving citizen data. As always, we are happy to assist with any part of such a project.

III. FREEDOM OF INFORMATION

As we noted earlier, FIPPA contains several exemptions to the right of access to records. These *include* the following notable examples: information that would reveal the substance of *in-camera* council or board deliberations (section 12(3)(b)); advice or recommendations (section 13); information that is subject to solicitor-client privilege (section 14); information the disclosure of which could reasonably be expected to harm a law enforcement matter (section 15); information the disclosure of which could reasonably be expected to harm the conduct of intergovernmental relations or reveal information received in confidence from another government (section 16); information the disclosure of which could reasonably be expected to harm the financial interests of the public body (or negotiations) (section 17); third-party financial information of certain kinds (section 21); and personal information the disclosure of which could reasonably be expected to unreasonably invade the personal privacy of an individual (section 22).[10]

This summary illustrates the breadth of the reasons for you to possibly refuse to disclose records. But you should keep the following things in mind.

First off, the default under FIPPA is, again, that you have to disclose any records that someone has asked for. If you think that one or more access exemptions applies – and quite often several apply to the same information – you have to apply the exemption to only those parts of a record that are protected. This is called severance (sometimes redaction) and FIPPA requires you to do this. You have to do a line-by-line review and only withhold the protected parts, which can sometimes be sentences, phrases or even words.

Another thing to keep in mind is that some exemptions are discretionary, some mandatory. And some are class exemptions, while others are harms-based exemptions.

Most of FIPPA's exemptions are discretionary. So, a local government "may", for example, refuse to disclose advice, or privileged information, but it is not required to. (The OIPC, may make you prove you considered exercising your discretion to disclose or note.) By contrast, a local government "must" refuse to disclose third-party business or personal information that meets the tests roughly summarized above.

[10] These are, of course, only rough summaries of the exemptions – refer to FIPPA's actual language in each case.

As the above summary suggests, some of FIPPA's exemptions are harms-based and some are class-based. The authority to withhold advice, for example, is a class exemption (section 13). If a record contains advice to a council or board, that exemption can be claimed without showing that disclosure would *harm* the deliberative process or some other interest. By contrast, some exemptions, such as the financial harm exemption (section 17), require proof of harm from disclosure of the information. So, a local government can only refuse to disclose information that it believes would harm its financial interests if disclosure "could reasonably be expected to [cause that] harm". The OIPC has for many years required – as have the courts – that public bodies provide pretty detailed evidence of harm for such a harms-based exemption to apply.

With this selective overview in mind, we will now review some recent leading cases in freedom of information.

A. Custody or Control of Records

The right of access only applies to records that are "in the custody or under the control" of the local government. There have been dozens of decisions over the years about the concepts of custody and control. The relevant factors for deciding whether a local government has custody or control of a record had been set out many times.

Recent decisions, from BC and elsewhere, illustrate how electronic information systems, including email, frequently figure in these decisions. In Order F18-45, for example, the OIPC had to decide whether the City of White Rock had custody or control of records about the City's connection to the Metro Vancouver Regional District water supply. As a member of a regional district utilities committee, the City's mayor had electronic access to regional district records. The OIPC accepted that, because the mayor only had access to those records in his capacity as a regional district committee member, and not in his capacity as mayor of the City, those records were not in the custody or control of the City and the access request for those records could be refused.[11]

Comparable cases have arisen in Alberta and Ontario. In *City of Ottawa v. Ontario*,[12] for example, the Court held that emails stored in a City employee's work email folder but relating solely to his volunteer work with a charity, were not in the City's custody or control. The City approved of the employee's volunteer activities using the City email system, and the fact that the emails were stored on City facilities did not matter.[13]

---

[11] Similarly, in Order F17-41, the OIPC ruled that the City of Vancouver did not have custody or control of records of a corporation it partly owned where the records were accessible only to a City councillor, who had been appointed to the corporation's board by the City.

[12] 2010 ONSC 6835 (CanLII).

[13] Also see *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2012 ABQB 247 (CanLII), where a university professor's emails about his volunteer work with a national organization were not in the University's custody or control simply because they were on the University's email servers. Ownership of the servers did not amount to custody or control of the emails for freedom of information purposes.

These cases illustrate the need for local governments to have clear and comprehensive policies on employee use of work email and other technology facilities, including use of the internet for personal purposes. Appropriate policies can help buttress your position in access appeals before the OIPC. They can also clarify your position on collection, use and disclosure of employees' personal information when they use your facilities for personal purposes.

B. *In-Camera* Deliberations (section 12(3)(b))

This provision allows a local government to refuse to disclose information "that would reveal…the substance of deliberations" of an *in-camera* council, board or committee meeting. The local government must provide evidence establishing these three things: there is statutory authority to meet in the absence of the public; the meeting was actually duly held in the absence of the public; and, the information in question would, if disclosed, reveal the substance of deliberations of the meeting.

Many decisions confirm that the OIPC closely scrutinizes whether each of these elements has been established. For example, in Order F19-18, the adjudicator spent a fair amount of time assessing whether section 90 of the *Community Charter* authorized the City of White Rock's council to meet *in-camera* to consider and pass a motion of censure against one of the councillors. The City relied on several subsections of that provision and, ultimately, the adjudicator decided that section 90(1)(i) applied.

Another recent OIPC decision affirms that, while *in-camera* meeting minutes may be withheld to the extent they would disclose the substance of actual deliberations – the "who said what" portion of minutes – deciding whether information would reveal the substance of actual deliberations is very much a case-by-case analysis. In Order F18-17, the adjudicator held that, while the *in-camera* meeting was properly held, the City of Parksville could not withhold – as information revealing the "substance of deliberations" – motions (including who moved and seconded each motion and who voted for each motion); headings within the minutes; and, a set of secondary headings revealing only the subject (not substance) of discussions.

C. Advice or Recommendations (section 13)

Section 13(1) authorizes a local government to refuse to disclose information "that would reveal advice or recommendations developed by or for" the local government. In recent years, court decisions have somewhat expanded the scope of this exemption, so that it can even extend to factual information that is an integral part of actual advice or recommendations.[14] In

[14] These decisions should be treated with some caution, however, including because section 13(2)(a) of FIPPA explicitly provides that a local government may not refuse, under section 13(1), to disclose "factual material".

Order F19-28, the OIPC upheld the City of Vancouver's reliance on section 13(1) to entirely withhold a letter that City staff had drafted for the mayor to consider sending. The adjudicator held that the letter amounted to advice or a recommendation to the mayor, since it had been prepared for him to consider sending. The adjudicator also upheld the City's refusal to disclose factual information contained in the letter, on the basis that this information was an integral part of the overall advice and recommendations.

D. Privilege (section 14)

There have been several decisions relating to section 14, which authorizes a local government to withhold information that is "subject to solicitor-client privilege". This covers both kinds of legal privilege, legal advice privilege and litigation privilege. In *Richmond (City) v. Campbell*,[15] the Supreme Court of British Columbia quashed a decision of the OIPC requiring the City to disclose records related to its settlement of wrongful dismissal claims by two former City employees. The Court ruled that information relating to the City's legal fees could be withheld (as do the other cases referred to below). The Court went further, however, in holding that, although FIPPA does not include an exemption for common law settlement privilege, FIPPA does not "contain express language that would abrogate settlement privilege and, accordingly, it should not be interpreted to have done so" (paragraph 72). The upshot was that records disclosing information about settlement negotiations could be withheld.

The OIPC did not appeal this decision, even though it is, with deference, quite clearly wrongly decided. As numerous decisions affirm, the right of access to records is subject only to the specified "limited exceptions to the rights of access" (FIPPA, section 2(1)(c)). Be that as it may, unless it is overturned down the road, *Richmond (City)* may be relied on to refuse to disclose records related to the settlement of legal disputes.

Two recent OIPC orders interpreting section 14 have been quashed by the British Columbia Supreme Court on judicial review. The first of these, *British Columbia (Attorney General) v. British Columbia (Information and Privacy Commissioner)*,[16] is the latest in a long line of cases in which applicants are seeking transparency about legal fees incurred by public bodies. In that case, the applicant sought "any and all records recording, describing or mentioning the cost of litigation to the Provincial Government" in a complex ongoing constitutional challenge by Cambie Surgeries Corporation of the *Medicare Protection Act*. In response to the request, the Ministry of Attorney General had created a record outlining the total cost of the litigation but withheld it in its entirety under section 14. The OIPC ruled, in Order F18-35, that the total cost of the litigation was not subject to solicitor-client privilege and ordered it to be released.

The Court overturned this decision, affirming that information about legal fees is presumptively protected by solicitor-client privilege. The Court clarified some ambiguities about whether facts can be separated from privileged communications and held that the presumption of privilege

[15] 2017 BCSC 331 (CanLII).
[16] 2019 BCSC 1132 (CanLII).

over the litigation cost had not been rebutted. The Court was apparently influenced by the fact that the litigation is ongoing – it remains to be seen whether a court would necessarily reach the same conclusion where the litigation has ended.

The second recent court decision is *British Columbia (Minister of Justice) v. British Columbia (Information and Privacy Commissioner)*.[17] In Order F-16-08, the adjudicator ordered the provincial Ministry of Justice to disclose an email from a lawyer with the federal Department of Justice to two lawyers from the Ministry and two other individuals on the basis that the email was not a communication between a lawyer and their client and did not contain a communication that was directly related to the seeking, formulating, or giving of legal advice. The Supreme Court of British Columbia held that the email was sent in the context of a solicitor-client relationship and that privilege applies to all communications made within that framework. This is certainly a broad interpretation of solicitor client privilege and this decision should not be seen as expanding the scope of privilege. The Court seems to have recognized the breadth of its decision, since it acknowledged that "not all communications from a lawyer are privileged" and also noted that policy advice, even from a lawyer, is not necessarily privileged.

A 2016 Supreme Court of Canada decision, *University of Calgary v. Alberta (Information and Privacy Commissioner)*,[18] has seen many members of the Canadian legal profession work themselves into quite a lather about the provision to information and privacy commissioners of records for which privilege is claimed. We of course recognize, and strongly defend, the vitally important principles of solicitor-client privilege. However, *University of Calgary* has been misinterpreted in many quarters and as a result can stand in the way of efficient and timely resolution of appeals to the OIPC by applicants who do not accept a local government's assertion of privilege under section 14.

University of Calgary involved an appeal to Alberta's Office of the Information and Privacy Commissioner in which the University had claimed privilege over some records. The adjudicator gave the University several opportunities to prove its privilege claim by providing information sufficient to establish privilege. The University refused to provide the records for review by the adjudicator and, ultimately, the adjudicator ordered their production for his review, under Alberta's *Freedom of Information and Protection of Privacy Act*. The Supreme Court of Canada ruled that the legislation was not sufficiently clear that the power to compel production of records applied where solicitor-client privilege was being claimed.

Despite claims of broad and sweeping implications, strictly speaking, this decision only deals with the language of the Alberta legislation and is not binding in British Columbia. This is illustrated by Order F19-21, a carefully and exhaustively reasoned OIPC decision involving a claim of privilege by the Ministry of Attorney General. That decision, which the provincial government has not challenged in court, concludes – having considered *University of Calgary*

[17] 2019 BCSC 1787 (CanLII).
[18] 2016 SCC 53 (CanLII).

and many other court decisions – that the OIPC has the power, under section 44 of FIPPA to compel public bodies to produce allegedly privileged records where it is necessary to "fairly decide" whether records are privileged under section 14 (paragraph 61).

The OIPC made it clear that it is preferable to adjudicate privilege disputes based on affidavit evidence: where a public body has provided sufficient evidence to substantiate its privilege claim, it is not appropriate for the OIPC to view the records as an additional check on the claim. Review of allegedly privileged records therefore will be limited to cases where there is doubt that the privileges have been properly claimed, or the evidence is inconclusive. It is also appropriate where affidavit evidence is insufficient to establish the privilege claim without revealing the privileged information itself. This decision reflects a restrained and nuanced approach to privilege claims, honouring the courts' caution around reviewing allegedly privileged records for which privilege has been claimed in civil litigation.

From a practical perspective, we continue to believe that local governments should, where their privilege claim has been challenged before the OIPC, attempt to persuade the OIPC that the privilege applies without routinely providing the records to the OIPC. This issue almost always arises in the course of the OIPC's attempts to resolve appeals without resorting to a formal inquiry and a formal order under FIPPA. We recommend that local governments first attempt to give the OIPC investigator sufficient information to enable the investigator to decide whether privilege likely applies, and then persuade the applicant, if possible, to drop that aspect of the appeal.[19]

A typical example of situations in which you should be able to provide the investigator with sufficient information is where a legal opinion from the local government's lawyers has been requested. It should be sufficient for the investigator's purposes for you to confirm that the record is a legal opinion provided to the local government by its lawyers. This information may be provided in an email (or sometimes telephone conversation).

In some cases, however, it may be necessary to provide the investigator with an affidavit sworn by a knowledgeable official of the local government. This is more likely in cases that do not involve a discrete legal opinion, such as cases where a lawyer has been copied in an email string and it is not feasible to sufficiently describe why that involvement cloaks the emails, in whole or in part, with privilege.

In any case, if an applicant is unwilling to concede the privilege point and the appeal proceeds to a formal inquiry, the local government should at that stage provide affidavit evidence to support the privilege claim. The affidavit should contain evidence that establishes each of the

[19] We note that the investigator does not disclose either the contents of the records, or the information provided by the local government, to the applicant. We also acknowledge that applicants may have unrealistic expectations about their access rights, but in our experience the OIPC is quite often able to resolve issues satisfactorily. This is a much more cost-effective approach to such disputes.

necessary elements of solicitor-client privilege (or litigation privilege).[20] If there is doubt about whether affidavit evidence will suffice, the privileged records can be provided to the OIPC adjudicator.[21] Where you submit affidavit evidence but not the records, your accompanying legal submissions should explicitly state that, if the adjudicator is not satisfied that the affidavit suffices, you request a further opportunity to establish the privilege, including by possibly providing the disputed records to the adjudicator.

To summarize, *University of Calgary* is not the game-changer that many lawyers have claimed, and it is in any case not the law in British Columbia. Order F19-21 establishes that the OIPC can, in appropriate circumstances, order production of allegedly privileged records where it is necessarily to fairly decide a privilege claim.[22] That decision also underscores the OIPC's appropriately balanced and cautious approach to these cases.

E. Confidential Bylaw Complaints (section 15(1)(d))

Many OIPC decisions have affirmed that a local government may refuse to disclose information that could reasonably be expected to "reveal the identity of a confidential source of law enforcement information". This invariably comes up when someone against whom a bylaw complaint has been made makes an access request to find out who lodged the complaint. In Order F15-18, the OIPC upheld the City of Kelowna's reliance on this section to refuse to disclose information that would reveal the identity of a bylaw complainant. The adjudicator, citing earlier OIPC decisions, noted that a local government may only rely on this exemption if it can establish that the complainant provided the information in confidence. He noted that the City's policy and procedures manual explicitly stated that a bylaw complainant's personal information would remain confidential unless it was needed for legal action on the complaint.

This decision underscores the benefit of having policies and procedures that specifically promise confidentiality for bylaw complainants. Of course, even if a local government does not have a confidentiality policy, it may be able to show that, in the specific circumstances, it gave the necessary confidentiality assurance. But it is undoubtedly preferable to have a policy that speaks to the confidentiality issue in all cases.

F. Negotiations About Community Amenity Contributions (section 17(1))

Under section 17(1), a local government may refuse to disclose information the disclosure of which could reasonably be expected to "harm the financial or economic interests" of the local government. Section 17(1) also contains several specific exemptions, including where the information is about negotiations carried on by the local government and where disclosure of

[20] Order F19-21 contains helpful reminders about what public bodies must do to satisfy their burden to prove their privilege claim.

[21] The OIPC of course never shares disputed records, including records for which privilege is claimed, with the applicant, as this would disclose the very information in dispute.

[22] Of course, is always possible that a future OIPC decision ordering production of allegedly privileged records will be successfully challenged in the courts, but for the time being, Order F19-21 is the law.

the information could reasonably be expected to harm the negotiating position of the local government. Section 17(1) has in the past been used to protect cost projections, land appraisals and financial information to be used in, or relating to, negotiations, as well as information about negotiating techniques, strategies, criteria, positions or objectives.

In Order F17-19, the OIPC upheld the City of Vancouver's reliance on section 17(1) in withholding a developer's proposal for community amenity contributions connected with the developer's rezoning application. The evidence established that these contributions are, strictly speaking, voluntary and that disclosure of the proposal would result in developers either no longer making such proposals, or in developers submitting much less detailed proposals. The adjudicator accepted that the necessary level of financial detail would not be available to the City in future development proposals. She placed "considerable weight on the evidence that developers do not have to pay" these contributions and "are not obliged to provide" them to the City as part of the negotiations on contributions (paragraph 40). She also accepted "that the results of the negotiations on the [contributions] in this case would have been less beneficial to the City if they had been based on less detailed, and thus less helpful, information than was included" in the developer's proposal (paragraph 41). Crucially, the adjudicator accepted "that the City's ability to negotiate optimal [contributions] in future developments could be harmed by lack of confidentiality and less detailed" proposals (paragraph 41).

G. Third Party Business Harm (section 21)

Among other things, section 21(1) of FIPPA authorizes a local government to, roughly summarized, refuse to disclose information that would reveal third-party business information that has been supplied in confidence, where the disclosure of that information could reasonably be expected to significantly harm the third-party's competitive position. For decades the OIPC has, with the support of the courts, taken a very strict line on the withholding of contracts entered into between public bodies and private sector suppliers or service providers. Many decisions have required disclosure of entire contracts, including unit and other pricing information.

Section 21(1) has, however, been used successfully to protect third-party information in other contexts. Order F18-07 is an example. In that case, the OIPC upheld the decision of the Metro Vancouver Regional District to withhold technical information that a business had supplied to it in support of its application for an emissions permit. The adjudicator accepted that information describing chemicals that the business used, details about the chemical processes that it employed and schematic flow designs relating to its operations qualified as "technical" information of the third party. She also found that the evidence established the necessary confidential supply of information and, finally, that disclosure would enable the business's competitors to get access to the processing information "without having to research, test and develop their own methods, as the third party was required to do", thus giving them an "undue financial…gain" under section 21(1)(c)(iii). The adjudicator upheld the decision to apply section 21(1).

H. Public Hearings: Best Practices

Public hearings can pose challenges in light of obligations under the *Community Charter*, the common law and FIPPA. On the one hand, the principles of transparency and openness require local governments to embrace new technologies such as live streaming of public hearings and the posting of materials online. On the other hand, FIPPA imposes fairly significant limitations on local governments around the collection, use and disclosure of personal information. Section 30.1 of FIPPA, notably, prohibits storage of or access to personal information outside Canada, which can present challenges for webcasting of hearings and meetings, and for website hosting of materials submitted by members of the public before a hearing or meeting. These competing duties can successfully work in parallel but there can be tension between them when, for example, the general public is invited to provide submissions or speak at a meeting and staff no longer have absolute control over what is said or submitted.

Regarding legal authority to collect personal information in this context, section 26(g) of FIPPA authorizes collection if the personal information "is collected by observation at a presentation, ceremony, performance, sports meet or similar event". Although this language could be clearer, our view is that a public meeting such as a council or board meeting, or public hearing, would likely qualify under this section. In that case, where a member of the public appears and provides personal information – such as their name and address, or their personal opinions about the matter – collection of other personal information is authorized.

Under section 32 of FIPPA, use of that personal information for the purpose for which it was collected would also be authorized. For example, if a municipal council was considering adopting a bylaw and members of the public express their personal opinions about the bylaw, the municipality would be entitled to use those opinions in revising the bylaw or adopting it.

Challenges can arise, however, where those personal views, and other personal information, are collected at a meeting or hearing that is being webcast. The challenge is that, as noted above, section 30.1 prohibits access to personal information from outside Canada. A webcast of a meeting or hearing necessarily involves making personal information available outside Canada. There are some exceptions to this rule that may be of assistance for webcasting of public hearings or meetings.

The most significant is section 33.1(1)(q), which authorizes the disclosure outside Canada of personal information that "is collected by observation at a presentation, ceremony, performance, sports meet or similar event".[23] As already noted, this language could be clearer, but our view is that a public meeting such as a council or board meeting, or public hearing, would likely qualify. In addition, section 33.1(1)(q) only applies if an individual whose personal information is collected voluntarily appeared and the meeting or hearing was open to the public. To help reduce the risk of a complaint to the OIPC, we generally suggest that local governments post clear notices at the entrances to the meeting or hearing. These should make it clear that the proceedings will be webcast, should state the legal authority under FIPPA for the collection, use, and disclosure of personal information, state the purposes for which the information will be used, and state that, by entering the meeting, individuals consent to their personal information being accessible outside Canada by virtue of the webcasting.

Another approach is to get the consent of each individual involved, since section 30.1(a) allows access from outside Canada if each individual whose personal information is stored or accessed outside Canada has consented. Because the consent must be in writing and must comply with the fairly detailed consent requirements under the *Freedom of Information and Protection of Privacy Regulation*, obtaining the consent of each individual obviously presents real administrative challenges in managing public hearings and meetings. Individual consent may, therefore, be the best approach from a strict legal perspective, but the practicalities are likely to drive local governments to rely on the above-described provisions, with notices being posted at hearings or meetings that are to be webcast – and notices on your website, as recommended below – to enable reliance on section 33.1(1)(q).

Another challenge can arise where meeting or hearing participants disclose personal information of other individuals in their written or verbal submissions to the public hearing or a meeting. Determining what can be included from materials that are made publicly available can be a difficult task for staff. As noted below, we recommend that local governments include, on their website pages relating to public hearings and meetings, information about including third-party personal information in submissions.

[23] Another exception that may apply is section 33.1(1)(c.1), which permits disclosure of personal information outside Canada if it is "made available to the public in British Columbia under an enactment other than FIPPA that authorizes or requires the information to be made public". The argument here would be that the *Community Charter* at least implicitly, in light of the case law on public hearings, both authorizes and requires local governments to make material submitted for public hearing, and submissions made at the hearing, "available to the public in British Columbia". A similar argument can be made about section 33.1(1)(c), which authorizes disclosure outside Canada "in accordance with an enactment of British Columbia, other than FIPPA, that authorizes or requires its disclosure." Neither of these arguments is a slam dunk, but they should be kept in mind if an individual complains to the OIPC.

Bearing in mind that the circumstances of each situation govern, we offer the following observations for the webcasting of meetings or hearings:

- You should place notices at the entrances to any meeting or hearing that is going to be webcast, noting the above considerations for the content of such notices;
- Review your local government's privacy-related information on your website, and ensure it describes your webcasting practices. Make sure this includes the above-noted notice about access to personal information outside Canada and the fact that individuals who provide their personal information are deemed to do so voluntarily for FIPPA purposes;
- Space permitting, consider posting the above information about webcasting on notice boards at your local government offices;
- Include this same information in published meeting and hearing notices if possible;
- At the outset of the meeting or before public input is solicited, have the chair:
  - Remind the audience that the meeting is being recorded and webcast globally and direct their attention to the notice;
  - Consider allowing individuals who do not wish to have their identity broadcast to provide their names and addresses to the clerk off-screen before speaking;
  - Noting the need to protect the privacy of others, state that personal information of third parties should only be provided if the individual providing it has been authorized to do so by the third parties; and
  - State that defamatory, obscene, or offensive language will not be tolerated and that the chair also reserves the right to control decorum.

I. Three Notable Cases

1. *BC (Attorney General) v. Fuller*[24]

This 2018 case was the first time that sections 73.1 and 73.2 of FIPPA were used by the provincial government on behalf of a public body to petition the Supreme Court of British Columbia for the return of personal information that a third party improperly obtained. Section 73.1 provides that if a public body has reasonable grounds to believe that personal information in the custody of or under the control of the public body is in the possession or a person or

[24] 2018 BCSC 1981 (CanLII).

entity not authorized by law to possess the information, the head can issue a notice demanding that person return the personal information. If that request is not successful, the public body may ask the Attorney General to petition the Court for the information's return or destruction.

The case dealt with emails the mayor of the City of Nanaimo had sent to a consultant and two letters written by a lawyer to the City of Nanaimo. Multiple parties, including a former City councillor and a member of the public, had obtained the records improperly. They were then published on social media and otherwise circulated. The City issued section 73.1 notices to the respondent councillors and the member of the public, demanding the return or destruction of the records. The respondents refused and the City asked the Attorney General to petition the Court under section 73.2.

The Court had little sympathy for the respondents. The Court confirmed that the City was still in control of the records and was entitled to issue the section 73.1 notices. The respondents were ordered to delete the records and return any copies to the City, as well as to delete any copies that they had transferred, published or disseminated on social media platforms to the extent they were reasonably capable of doing so. Finally, the Court ordered costs against the respondents in favour of the Attorney General.

This case illustrates how challenging matters can be where the individual responsible for the breach is a sitting councillor. Fortunately, the provincial government was prepared to step in to assist the City in this case, and the Court's decision underscores that sections 73.1 and 73.2 should be kept in mind even when faced with such challenging circumstances.

2. *McAlister v. Calgary (City)*[25]

In *McAlister v. Calgary (City*), the plaintiff and a woman were walking across an overpass attached to the City's urban rail system. The overpass was monitored by City staff using live CCTV. The plaintiff and the woman encountered the woman's ex-boyfriend. The plaintiff was violently assaulted by the former boyfriend and his friend and suffered severe injuries over the course of a 20-minute assault.

The trial judge found that the City was an occupier of the overpass, that the plaintiff was a visitor and the City owed him a duty of care. At the time of the assault, on New Year's Eve, two City employees were watching 42 CCTV monitors, which cycled through 337 cameras, 25 of which were near the station where the assault occurred. The trial judge held this was insufficient – the assault should have been detected within the first minute and help should have been dispatched sooner. Had that been done, the court found, the plaintiff's injuries would have been less severe. The City was held liable in damages.

[25] 2019 ABCA 214 (CanLII).

The Alberta Court of Appeal narrowed the trial decision, but still held that the City was in breach of its duty for failing "to have in place reasonable systems for detecting and responding to the assault on the respondent. As such the City is liable for the incremental damages suffered by the respondent, after the reasonable response time of ten minutes".[26]

Both the trial and appeal decisions could have far-reaching implications for local governments that already have or are considering implementing live-monitored CCTV cameras in areas where the local government is an "occupier" of "premises" under the *Occupiers Liability Act* (and perhaps areas where the local government is not an "occupier"). The risk is that, in essence, the expectation of protection where CCTV is present may have financial consequences for local governments if that expectation is not met. An application for leave to the Supreme Court of Canada has been filed by the City of Calgary and was submitted to the Court for consideration on October 28, 2019.

3. *Raymond v. Nova Scotia (Information and Privacy Commissioner)*[27]

This case boils down to whether a request under access legislation must be a request for records, as to a request for information. The applicant was apparently aware that the right of access under relevant legislation was a right of access to records and that the legislation would exempt council meeting minutes from disclosure. She therefore framed her request to the Halifax Regional Municipality as a request for whether herself or her property had been the subject of discussions at a closed meeting of the regional council.

The Nova Scotia Court of Appeal noted that the applicant knew that the records, which she could not obtain under the access legislation, existed and that she had therefore framed her application as a request for information, not records. She sought to construct her application as an application for "personal information" and argued that she had a right to know if she had been the subject of discussion at an *in-camera* council meeting, a right that should "trump" the confidentiality protections that apply to such meetings. The Court was not impressed and upheld the decision that the request fell outside the legislation, which provides a right of access to records, not information. This case is a helpful reminder that local governments are entitled to ask applicants to re-frame requests for information as requests for records.

IV. OIPC UPDATE

Two OIPC publications deserve brief discussion.

[26] Paragraph 81.
[27] 2019 NSCA 1 (CanLII).

A. City of White Rock Audit and Compliance Report F18-02

Under section 42 of FIPPA, the OIPC may conduct investigations and audits to ensure compliance with any provision of FIPPA. The OIPC reviewed the City of Vancouver's freedom of information processes in 2016, under the guise of a review of the duty to assist access applicants.[28] The OIPC's continued interest in local government compliance is demonstrated by, among other things, Audit and Compliance Report F18-02, an audit and compliance review of the City of White Rock, which was prompted by the numbers of requests for reviews and complaints to the OIPC relating to the City.

The audit evaluated the City's handling of access requests in 2016 and 2017. It found that the City did not meet legislated timelines in 46% of sampled files and took on average 38 days to respond, with an average of 13 days to forward requests to relevant City departments. Also highlighted was the fact that the City took on average 22 days longer to respond to recurring applicants, defined in the report as applicants who submitted 5 or more requests in a calendar year.

While the report did find that the City conducted adequate searches for records, rarely applied fees, and generally released records with little or no severing, the OIPC recommended that the City: fully document all FOI requests, from the original request to the closing of the file; forward access requests to departments to search for records as soon as possible; and respond to all access requests without delay and within legislated timelines.

The OIPC also noted that, while resource issues may have had an impact on the City's responses, the lack of resources does not excuse compliance with the law. The OIPC again emphasized that local governments must provide sufficient resources for their FIPPA obligations, to ensure they fulfill their legislated mandate.

B. OIPC Guidance on Public Interest Disclosure (section 25)

Last December, the OIPC released guidance on how to interpret and apply what is commonly referred to as the "public interest override", found in section 25 of FIPPA. This guidance builds on the important interpretive direction from the OIPC in 2016, which overturned 20 years of interpretation of the public interest override.[29]

Section 25 has two branches, each of which requires public bodies to disclose information, even if no access request has been made and despite any of FIPPA's exemptions from disclosure. We are concerned here with the second branch, which requires disclosure of information "the disclosure of which is, for any other reason, clearly in the public interest" (section 25(1)(b)).[30]

[28] Audit and Compliance Report F16-01.
[29] Investigation Report F16-02.
[30] The first branch requires disclosure to the public or an affected group of people of information "about a risk of significant harm to the environment or to the health or safety of the public or a group of people" (section 25(1)(a)).

The OIPC has held that public bodies must disclose information proactively "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".[31] The non-exhaustive list of factors that public bodies should consider include whether the information would contribute to educating the public about the matter, would contribute in a substantive way to the body of information already available about the matter, or would contribute in a meaningful way to holding a public body accountable for its actions or decisions. Public bodies may also weigh the interests protected by any applicable disclosure exemptions.[32]

Turning to the 2018 OIPC guidance on applying section 25(1), the guidance affirms that section 25 applies to information, not just records. This is particularly relevant for section 25(1)(a), which imposes a duty on local governments to disclose information about a risk of significant harm to the environment or to the health or safety of the public or a group of people. Even if the local government does not possess a record that comprehensively describes the risk, it still has a duty to disclose information contained in one or more records where the section has been satisfied. For example, if a public body has in its possession a complex geotechnical report showing a risk to a group of residents, it need not release the entire report but would need to warn those individuals about the risk if section 25(1)(a) is satisfied.

As for implementation, the guidance offers useful suggestions on how to comply, notably the need for an organized process through which individual staff members can bring potentially relevant information to the head of the public body for assessment of whether to release. The OIPC suggests creating criteria for determining what constitutes a risk of significant harm and for determining if disclosure is clearly in the public interest. Of note is also the requirements under sections 25(3) and 25(4).

V. CONCLUSION

The goal of this paper has been to canvass selected key developments in access and privacy over the past few years. As these developments indicate, there have been some significant developments in British Columbia, and elsewhere, and the coming years will no doubt offer more of the same.

[31] Investigation Report F16-02, at page 29.
[32] Investigation Report F16-02, at page 38.

NOTES