YOUNG ANDERSON
BARRISTERS & SOLICITORS

# WHAT'S NEW IN THE WORLD OF FREEDOM OF INFORMATION?

## NOVEMBER 26, 2021

*[David Loukidelis, Amy O'Connor, and James Barth]*

# WHAT'S NEW IN THE WORLD OF FREEDOM OF INFORMATION?

## I. INTRODUCTION

The law and procedure surrounding freedom of information ("FOI") is in a constant state of flux. Its state of play continues to be altered both incrementally and by sudden sea-change. Gradual change typically flows from consequential legislative amendments, decisions of the Office of the Information & Privacy Commissioner ("OIPC"), court rulings, and less formally through guidance and best practice documents. Our ever-changing FOI law shows that it adapts to new circumstances and challenges, but this malleability can make it an uncertain and challenging area for local governments. This paper will address some of these uncertainties and challenges and offer tips on some complex areas of the current regime, namely, how to manage vexatious requesters, issues with giving third parties' notice of requests, and handling commercial applicants.

Sea changes in the law are typically legislative, and Bill 22 – 2021: *Freedom of Information and Protection of Privacy Amendment Act, 2021* ("Bill 22") has British Columbia on the precipice of a major shift to the topography of FOI. If passed, Bill 22 will significantly change the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), the central piece of legislation governing FOI for local governments. This paper outlines the amendments proposed in Bill 22, with particular attention to key areas of change relevant to local governments' interests and operations.

## II. BILL 22 – MAJOR SHIFTS IN THE FIPPA FRAMEWORK

### A. Bill 22 – An Overview

The need for an ongoing review of the legislative regime is recognized in FIPPA itself. Section 80 requires a comprehensive review of FIPPA by a special committee of the Legislative Assembly at least once every six years. There have been several reviews—most recently, in 2015—but none of them has led to significant updates. The current review committee was appointed on June 16, 2021; it has met once, for 15 minutes, to appoint a chair and vice-chair.

Although the special committee has not started to actively pursue the review, the provincial government has gone ahead with Bill 22, which was tabled on October 18, 2021. Many observers, and the official opposition, have criticized the government for pre-empting the statutory review, especially because Bill 22 will make the most significant changes to FIPPA since it was enacted. The proposals themselves have provoked heated discussion and opposition, by advocacy groups, and in the media and the Legislative Assembly.

Several of the proposed changes are particularly worthy of attention and are discussed below. These are the introduction of access request application fees; the removal of in-Canada storage requirements; privacy breach notification rules; the requirement to have a privacy management plan; creation of new offences; and the addition of new grounds to disregard access requests.

### B. Bill 22 – Privacy Management Programs

Bill 22 will require local governments and other public bodies to "develop a privacy management program for the public body … in accordance with the directions of the minister responsible for this Act" (new section 36.2 of FIPPA). It is hard to predict what the ministerial directions will require, of course. It is reasonable to suggest to proactive local governments that the OIPC's best practices guidance for privacy management programs reflects the core of what will be required.[1] Best practices include designating a privacy officer responsible for directing the program; conducting ongoing compliance reporting and internal audits; developing and maintaining a personal information inventory; and assessing the risks of any new projects that may involve the collection of personal information. Employee training will also be an important part of a successful program.

Although the requirement for a privacy management plan will impose additional operational burdens, when properly designed and implemented they can reduce costs by making privacy compliance more efficient and ideally by reducing the risks of privacy breaches, which are expensive to deal with. Any reduction in the risk of privacy breaches can be particularly cost-effective in light of Bill 22's scheme for privacy breach notices.

### C. Bill 22 – Privacy Breaches

A new section 36.3 of FIPPA will require public bodies to notify affected individuals, and the OIPC, of certain privacy breaches. It will define a "privacy breach" as the theft or loss, or the collection, use or disclosure of personal information, that is not authorized by Part 3 of FIPPA. If a breach could reasonably be expected to result in "significant harm" (including a number of specified physical, reputational, and financial harms) to the affected individual, the public body must notify the affected individual and the OIPC "without unreasonable delay".

[1] See for example "Accountable Privacy Management in BC's Public Sector", Office of the Information & Privacy Commissioner, 2013 <https://www.oipc.bc.ca/guidance-documents/1545>; "Getting Accountability Right with a Privacy Management Program", Offices of the Information and Privacy Commissioners of Alberta and BC, 2012 <https://www.oipc.bc.ca/guidance-documents/1435>.

As media reports regularly show, privacy breaches—whether accidental or due to hacking—can involve hundreds or even thousands of individuals. Although the OIPC conceivably might support a general, broadcast notification to all affected individuals, in many cases each affected individual will have to be notified. The cost can be substantial. As can be the cost of stemming the breach, mitigating any losses, restoring information systems, and implementing appropriate fixes to prevent similar breaches down the road. The cost of reputational damage, and possible political fallout, can also be very real, if not monetarily quantifiable. The best approach, therefore, is to take every reasonable step to prevent breaches in the first place, including through your privacy management plan.

### D. Bill 22 – Privacy Impact Assessments

Bill 22 will also provide welcome clarity about local governments' responsibility to conduct privacy impact assessments ("PIAs"). The current section 69(5.3) of FIPPA is unclear about whether local governments have a positive duty to conduct PIAs. Bill 22 will clear this up, removing doubt about whether this positive obligation exists.

Bill 22 will also add a new section 69(10), empowering the minister to give specific directions as to what PIAs will require depending on the category of personal information.

This top-down approach, with the provincial government imposing duties on local governments, may not be universally welcome, but there is hope that the ministerial directions on PIAs, differentiated by types of personal information, can better support PIAs.

It bears underscoring that PIAs are to be conducted at the earliest practicable stage of project design, which helps ensure that expensive capital or operational decisions are made based on a clear understanding of compliance implications and their costs. It also bears repeating that PIAs will in many cases be straightforward, since the threshold question is whether personal information is involved at all. If it is not, that is the end of the exercise. A final reminder is that PIAs are most useful, especially in an information-systems setting, if they are treated as evergreen, with system or program updates being assessed by updating the PIA.

### E. Bill 22 – New Offences

From the outset, FIPPA's default approach to oversight and enforcement has been through the OIPC's investigation and audit powers. In the privacy sphere, the remedies have quite consistently taken the form of recommendations for reform. This will continue after Bill 22, but the Bill will introduce a more robust, penal approach to privacy compliance (and to FOI compliance).

For freedom of information, the proposed section 65.3 will make it an offence to "willfully" conceal, destroy or alter a record in an attempt to avoid complying with an access request. Individuals who violate this section will face a fine of up to $50,000. Corporations will face a fine of up to $500,000.

On the privacy side of the ledger, a new section 65.4 will make it an offence for an individual—or a service provider (a person contracted by a public body to perform a service) or its employees—to "wilfully" collect, use, or disclose personal information except as authorized by Part 3 of FIPPA. The fines for offences are the same as for records destruction.

An obvious aim of this offence is to deter snooping into other people's personal information. Alberta's OIPC has secured at least 19 convictions of individuals for a similar offence in that province's *Health Information Act*, with fines ranging as high as $20,000. Fines are not the only likely sanction for those caught snooping, since job loss or demotion is likely to ensue as well.

A well designed and implemented privacy management program—and effective access management controls for information systems—can help prevent these offences, as well as reduce instances of privacy breaches.

### F. Bill 22 – Disclosure Exceptions

A significant new mandatory access to information exception is also contained in Bill 22. This exception comes from the addition of section 18.1, "disclosure harmful to interest of an Indigenous people", which will require public bodies to refuse to disclose information if that disclosure could reasonably be expected to harm the Indigenous people's rights regarding their cultural heritage; traditional knowledge and cultural expressions; or manifestations of sciences, technologies or cultures. This exception would not apply, however, in the event that the affected Indigenous people have given written consent to the disclosure in question. Section 18.1 will also be a further ground for providing third-party notice under section 23. The details of third-party notice requirements are discussed below.

Bill 22 also adds new language to section 3 of FIPPA, which sets out the scope of the Act's application. The new section 3(5) will exclude the right to access several forms of information: records available for purchase by the public; records that do not relate to the public body's "business"; metadata describing an individual's interaction with an electronic system; and "lawfully" deleted electronic records. While it remains to be seen exactly how these new exclusions will be applied, some conjecture is possible about what information may be excluded from the right of access. The metadata exemption would appear to mean that it will no longer be possible through an access request to see who edited a particular document, what changes and revisions were made, and the history of when these changes were made. The "lawfully deleted" exclusion means that if a local government's record retention rules—and any other applicable requirements, e.g., in statute—allow an employee to delete emails from their system account such that the employee can no longer access them, they will no longer be subject to disclosure (even if copies could conceivably be recovered from a backup server). Lastly, while it obviously remains to be seen how the OIPC will interpret the exclusion of any "record that does not relate to the business of the public body", it clearly has the potential to be very broad.

## G. Bill 22 – Application Fees

A highly contentious aspect of Bill 22 seems to be the proposed addition of prescribed application fees, i.e., fees that can be charged to someone for making an access request. Commissioner Michael McEvoy, the media, many advocacy groups and others have been severely critical of this change. The Bill 22 clause implementing this new fee has been approved in the Legislative Assembly, however, and appears headed for the statute books.

This new fee will supplement the existing fee scheme under section 75 of FIPPA. That section allows a public body to charge the fees set out in the FIPPA regulations for specified services in responding to requests, i.e., locating, retrieving and producing the record; preparing the record for disclosure; shipping and handling the record; and providing a copy of the record. Bill 22's proposed section 75 will work by permitting public bodies to charge a prescribed fee for the initial application itself, in addition to the existing service fees.

The application fee has not been set, as it will be set by regulation, but in legislative debate the range of $5 to $50 in other jurisdictions has been mentioned, as has a fee in the middle of that range. These fees will not apply to applicants who are requesting disclosure of their own personal information.

Applicant fees may assist in reducing the overall number of incoming requests and help offset costs associated with request processing and document disclosure, having the potential to be a valuable tool for local governments in managing an overtaxed FOI system.

## H. Bill 22 – In-Canada Requirements

Bill 22's removal of the in-Canada data storage and access requirements will be a seismic shift in the public sector privacy landscape. Section 30.1 of FIPPA requires public bodies to ensure that personal information in their custody or control is stored and accessed solely in Canada. While there are exceptions in sections 30.1 and 33.1(1)—and amendments in 2019 eased the restrictions somewhat further—the in-Canada rule has hindered, if not outright prevented, local governments seeking to adopt innovative technologies to better serve citizens. The benefits of cloud technologies—including software-as-a-service solutions, data storage, videoconferencing and telecommunications services—have been beyond reach or immensely expensive to implement.

Bill 22 will repeal the core in-Canada provision, section 30.1, and allow for disclosure of personal information outside Canada. A new section 33.1, however, will provide that this may be done "only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for" FIPPA. As is the case with the privacy management and PIA provisions, we will have to wait to see what the regulations require. Our expectation is that they will require PIAs to be conducted—including to assess the strength of privacy protections in a foreign country—and require technical or contractual measures to protect personal information outside Canada.

If the in-Canada residency requirement is removed, local governments should carefully consider what personal information they store or disclose outside Canada, whether or not regulations are made. Not all personal information is created equal, and context is essential – rather than adopting an all-or-nothing approach to external storage and disclosure, it will be important to assess the risks and benefits for migrating information to non-domestic services. This assessment will help local governments ensure that they meet their duty under section 30, which will be unaffected by the Bill 22 changes, to implement reasonable security measures to protect personal information from risks such as hacking or inappropriate disclosure to authorities outside Canada.

### I. Bill 22 – Section 43 Grounds to Disregard Access Requests

Bill 22 would also add two significant new avenues for public bodies to seek permission to disregard certain requests under section 43 of FIPPA. Section 43 now allows a public body to ask that the Commissioner authorize it to disregard access requests where it can demonstrate that the requests in question are frivolous or vexatious, or that they are repetitious or systematic to such an extent that fulfilling the requests would unreasonably interfere with the public body's operations. Thus, section 43 provides an important remedy for local governments to deal with vexatious or overburdening applicants; however, the application of this section in practice can be limited, as this paper discusses further below.

If Bill 22 is passed, section 43 will also allow for the authorization to disregard requests where the requested record is available elsewhere, or where the request is so broad in scope that it would unreasonably interfere with the public body's operations. For the first, a public body must demonstrate that the requested record has previously been disclosed to the applicant, or that it is accessible through another source. Local governments may be able to employ this section in circumstances where applicants are not availing themselves of publicly available records. However, if a local government wishes to rely on this ground to disregard requests, it should ensure that the available records are directly responsive to the applicant's specific request, and are not merely generally relevant, or related information.

The second new ground would provide an avenue for public bodies to disregard a request which is excessively broad. Local governments may look to this section if initial attempts to get the applicant to refine the request are unsuccessful.

## III. NAVIGATING FIPPA

### A. Update – Systematic and Vexatious Requesters

Speaking of section 43, we recognize that it can be challenging to navigate and that the OIPC continues to set a very high—some would say excessively onerous—standard for relief. Recent OIPC decisions demonstrate this, as we will outline in a moment.

It is first worth recalling that, even when granted, section 43 relief often applies to only some of the requests involved, rather than allowing the public body to ignore all of them. More positively, relief may sometimes also be prospective, rather than being limited to current requests. However, prospective relief is invariably time-limited, and often for a year or rarely two. The OIPC also may permit a public body to have to respond to a small number of requests in that time, and even set maximum hours that the public body has to spend on them.

As already noted, however, the threshold for relief under section 43 is very high, some say exceedingly stringent, as two OIPC decisions this year show.

The first decision is *City of Nanaimo*, 2021 BCIPC 02,[2] which imposes strict evidentiary requirements on public bodies seeking relief under section 43. In *Nanaimo* the respondent, a former City employee, had filed a complaint with the BC Human Rights Tribunal against the City and two additional individuals. The respondent made a series of FOI requests to the City. The first three, made between May and June 2020, were fulfilled by the City without contention. Between August and September of 2020, the respondent made a series of further requests for correspondence between the City and its accounting firm, union, and select City employees, as well as copies of forensic audit reports. Between the fulfilled requests and subsequent submissions, the applicant made a total of 23 individual access requests. In response to this second wave of requests, the City applied for relief under section 43 which would limit the respondent to one active request at a time, with no more than 5 hours of staff time required per request.

The City's application for section 43 relief was denied. The adjudicator held that the respondent's requests were not repetitious or systematic, finding that the fact that one request was connected to a previous one did not inherently demonstrate repetition. The adjudicator also required clear evidence of what records had previously been disclosed to the applicant before deciding whether these requests were systematic. This second requirement places a demanding standard on local governments seeking relief, potentially requiring the disclosure of large amounts of previous records, from past requests by the same person, to the OIPC for review.

The adjudicator also did not find the respondent's requests to be frivolous or vexatious. The City alleged the respondent had previously abused the FOI process, and engaged in a slew of hostile behaviour towards City staff. The adjudicator noted that, even if all the City's allegations were substantiated, there was a limit to the extent which the respondent's past conduct could be considered, as it was still possible her subsequent requests were made in good faith. Much of the City's evidence regarding the respondent's abusive conduct was given *in camera.* While the adjudicator acknowledged this evidence helped provide context, the adjudicator placed

[2] These citations are from CanLII, and they allow you to find OIPC decisions for free, by entering the citation at www.canlii.org. All OIPC decisions since 1994—the first year of OIPC decisions—are found on CanLII.

limited weight on it as the respondent could not know and respond to the details of the allegations against her. This is somewhat troubling because the OIPC had given the City permission to submit that evidence *in camera* in the first place, and the adjudicator did not give the City any notice that less weight would be put on the evidence because it was *in camera*.

The second decision is *District of Kent*, 2021 BCIPC 39, which indicates that the OIPC may give limited weight to withdrawn requests when considering relief under section 43. In *Kent*, the respondent, a former employee, had resigned from her position due to an allegedly toxic work environment. The respondent made 12 initial access requests, all of which were fulfilled by the District. An additional 59 requests were then made in a one-month period and the District sought section 43 relief for those requests.

In the time between the District filing its section 43 application and the adjudicator issuing a decision, the respondent withdrew all but 14 of these requests. In denying relief, the adjudicator assessed only the remaining 14 requests, stating that the withdrawn requests could provide context for the analysis, but were not subject to section 43 themselves. The high volume of requests submitted by the respondent was acknowledged, and the adjudicator noted that, had the majority of the requests not been withdrawn, some degree of section 43 relief would have been granted. The adjudicator also acknowledged the District's concern that the respondent would simply reapply for the withdrawn requests once the proceedings were over. The adjudicator nonetheless suggested that the District's recourse would be to apply for section 43 relief all over again. This is problematic because it puts local governments in the unenviable position of potentially having to deal with vexatious applicants who tactically make and withdraw large swathes of requests, in a never-ending cycle of abuse of the right of access to records.

It would be troubling if *Nanaimo* and *Kent* indicate a trend towards further increasing the already high threshold for accessing section 43 relief. Local governments looking to invoke this provision should ensure they have as much clear evidence as possible of the burden requests are placing on their operations; the applicant's ongoing vexatious intent; and prior document disclosure to the applicant. Local governments may hope that Bill 22's expansion of section 43 will ease this burden, but for the moment it appears that relief is reserved for only the most egregious, outrageous cases, which is a matter of some concern.

## B. Update – Third Party Requests

Another area that can be fraught with difficulties for local governments is determining when to formally notify third parties, under section 23 of FIPPA, of access requests that may affect them.[3]

Section 23 only applies where information that may be protected under either section 21 or 22, which we discuss below, is involved. If a public body intends to disclose information that might be protected under either of these provisions, section 23(1) says it *must* give the "third party"[4] written notice of the request. The section specifies what the notice must say, and section 24 sets out timelines for the third party's response and the public body's decision. Further, section 23(2) allows a public body to notify a third party of the request even where the public body intends to refuse disclosure of the information. Third party input can be useful in making the right decision on disclosure, and a third party may even consent to disclosure of information that the public body has decided it must withhold.[5]

## C. Update - Section 21

This provision aims to protect what might usefully be called the "business interests" of third parties who routinely deal with local governments and other public bodies. Businesses may, for example, provide confidential commercial information to a public body as part of a procurement process, or to help with planning or economic development initiatives. Such information can be valuable for competitors, who may make an access request to get at it.

There are three elements to the section 21(1) protection for third party business interests. First, there has to be information that would reveal trade secrets, commercial, financial, labour relations, scientific or technical information of or about a third party. Second, the information must have been supplied to the public body (either implicitly or explicitly) in confidence. Third, disclosure must be reasonably expected to result in any of three types of harm specified in section 21(1)(c). If all three parts of the test are met, the public body *must* refuse disclosure of the protected information.

[3] Of course, local governments may consult other public bodies or institutions informally, even where section 23 does not technically apply. For example, a local government might consult the provincial government about whether disclosure of information would, under section 16(1)(a), harm the conduct relations between the two governments. This kind of consultation is not formally required under section 23 but can improve decision-making.

[4] Schedule 1 to FIPPA defines "third party" as, in relation to an access request, "any person, group of persons or organization other than…the person who made the request, or…a public body".

[5] Both sections 21 and 22 permit disclosure of otherwise protected information where the third party consents to disclosure.

A perennially challenging aspect of this test is determining what counts as "supplied" information. For decades now the OIPC has consistently affirmed that information in a contract—including, for example, unit pricing—will not normally qualify as "supplied" because it is the product of negotiations, or is susceptible to change through negotiations, and thus is not truly "supplied" by the third party.[6] Some recent OIPC decisions provide helpful guidance on this element of the test.

In *British Columbia Institute of Technology*, 2020 BCIPC 64, BCIT refused to disclose a third party's bid to provide health and welfare benefits. The adjudicator discussed what constitutes "supplied" information, noting that information in a contract will not normally qualify as supplied, as it is the product of the negotiations and modifications by both parties, not supplied unilaterally by one side. The adjudicator helpfully noted two exceptions where contractual information is nonetheless considered "supplied": where the information is non-negotiable (for example fixed labour or other overhead costs), and where the information would allow someone to draw an accurate inference about underlying "supplied" confidential information.

Another recent decision, *BC Pavilion Corporation*, 2021 BCIPC 37, further distinguishes between "supplied" and "negotiated" information. The adjudicator noted that information being that the fact that one party alone provided the information does not of necessity make it "supplied":

> Information may be delivered by a single party or the contractual terms may be initially drafted by only one party, but that information or those terms are negotiated and not "supplied" if the other party must agree to them in order for the agreement to proceed.

Lastly, *City of Vancouver*, 2021 BCIPC 19, noted that confidential information can be supplied to the public body by someone other than the third party and still be exempt under section 21. The initial source of the information does not matter, so long as it meets all the requirements of the test: it is business information, it was supplied in confidence, and its disclosure would harm the third party.

## D. Update - Section 22

Section 22(1) requires public bodies to refuse to disclose personal information where the disclosure "would be an unreasonable invasion of a third party's personal privacy".[7]

[6] The courts have upheld this interpretation on several occasions.

[7] This language implies that there may be "reasonable" invasions of privacy, and that only "personal" privacy is being protected. That is a conversation for another day.

It has long been accepted that the section 22(1) analysis involves four steps. First, it must be determined whether the information in dispute is in fact "personal information", which FIPPA defines as "recorded information about an identifiable individual other than contact information".[8] Second, the public body must consider whether the information, or disclosure, falls under any of the several section 22(4) tests. This is the second step because section 22(4) says that disclosure "is not" an unreasonable invasion of personal privacy where it applies. An example is where the "information is about expenses incurred by the third party while travelling at the expense of a public body". Another example is where the information is about the third party's "remuneration", such as salary and benefits.

If section 22(4) does not apply, the third part of the test involves deciding whether any aspects of section 22(3)'s ten "presumed" unreasonable invasions of personal privacy apply. Examples include where the information relates to medical history, educational history or employment history.

The fourth and final step involves considering "all relevant circumstances"—including those found in section 22(2)—in deciding whether disclosure of the personal information would unreasonably invade the third party's personal privacy. This analysis applies even if a section 22(3) presumption does not apply.

Two recent OIPC decisions illustrate the nuance and sometimes tricky balancing involved in determining whether personal information must be withheld under section 22. First, *BC Transit*, 2021 BCIPC 22, helps distinguish between exempt and non-exempt employment information. The adjudicator noted that the context of where the disputed information appears is crucial. An employee's name is normally information about their work position or functions and therefore, under section 22(4)(e), its disclosure *is not* an unreasonable invasion of personal privacy. As *BC Transit* affirms, however, if the same employee's name is listed in the context of an investigation into their workplace conduct, it *is* part of their employment history, and its disclosure is presumed under section 22(3)(d) to be an unreasonable invasion of personal privacy.

[8] Schedule 1 defines "contact information" as "information to enable an individual at a place of business to be contacted", including the individual's name, position name or title, and the individual's business phone, email, fax and address.

Another useful example is *University of British Columbia*, 2021 BCIPC 36, which also dealt with the context of a workplace investigation. The adjudicator noted that disclosure of objective, factual statements about what a third party (in this case, a former UBC employee) did or said in the normal course of their duty is not an unreasonable invasion of personal privacy. However, disclosure of qualitative assessments or evaluations of those actions during the normal course of duty, such as those made by an investigator during an evaluation, may constitute an unreasonable invasion of personal privacy.

### E. Update – Commercial Applicants

Another occasionally thorny area for local governments is determining who meets the definition of a "commercial" access applicant and what rules apply to them. The starting point for these questions is the *Freedom of Information and Protection of Privacy Regulation*. The regulation defines a "commercial applicant" as "a person who makes a request for access to a record to obtain information for use in connection with a trade, business, profession or other venture for profit". This definition is broad and outcome-focused: if the goal of the application is to use the information in a way that is connected to commercial gain, the requestor could be considered a commercial applicant. It can of course be difficult to know at the outset whether an applicant meets this test. The public body might, for example, only have the name of an organization or firm associated with the applicant to go by and the applicant might well be unwilling to offer any clarification to help make this decision. This can raise difficulties because, on any appeal to the OIPC, the onus is on the local government to establish that the applicant is a "commercial" applicant. We suggest that some common categories of applicants that you might consider to be "commercial" in nature are development companies, lawyers, and insurance adjusters.

Commercial applicants can be charged fees equivalent to "the actual cost to the public body of providing that service". As determining the actual cost of each individual service can be burdensome, some local governments charge a flat rate of $30 per hour of staff time spent on a commercial applicant's request. It is important to note however, that there is discretion to charge a commercial applicant actual cost or charge the fees set out in Schedule 1 to the regulation, once one or the other has been selected you cannot mix and match rates. As was well stated in *Law Society of British Columbia*, 2009 CanLII 21404:

> Public bodies to which the Regulation applies must choose either the Schedule or the "actual cost" (whatever it is) in calculating fees. It is not open to them to pick and choose, à la carte fashion, among the fees payable by "commercial" and "other" applicants.

As noted earlier, Bill 22 will enable application fees to be prescribed by regulation. The Schedule 1 list of fees has not really been changed since FIPPA came into force, so it is possible that it will be updated in the process of prescribing a new application fee. This would certainly be a welcome development, although there is always risk when a regulation is opened up.

## IV. CONCLUSION

As this paper illustrates, freedom of information is an ever-changing area of law and practice and Bill 22 means there are significant changes on the horizon. These changes are being hotly debated in the Legislative Assembly at the time of writing, so it remains to be seen what the amendments ultimately will look like. We have, however, offered our take on the nature and likely impact of several of the proposed changes, principally the removal of data residency requirements; new duties around privacy management and privacy breaches; exclusions of some types of records; and the expansion of section 43, all of which will significantly shake up the FOI framework.

In the meantime, many aspects of this law continue to incrementally shift, as the discussion of notifying third parties, applying for relief against vexatious applicants and practices around defining and charging commercial applicants show. British Columbia is on the precipice of the biggest shift in access and privacy law in well over a decade. While that sea-change will create some uncertainty as local governments seek to understand and implement the changes, we believe it will also create opportunities for a more efficient, accessible, and flexible approach to privacy and access and to doing business at the local level.

## NOTES

**NOTES**