YOUNG ANDERSON
BARRISTERS & SOLICITORS

FOI & PRIVACY LAW UPDATE

NOVEMBER 24, 2023

Amy O'Connor and James Barth

FOI & PRIVACY LAW UPDATE

I. INTRODUCTION

The legal landscape around freedom of information ("FOI") and privacy in British Columbia was altered significantly in late 2021. The Province passed the *Freedom of Information and Protection of Privacy Amendment Act, 2021* ("Bill 22"), which contained significant additions and changes to the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), the central piece of legislation that governs FOI and privacy for local governments and other public bodies. Some of these changes were instantaneous, coming into force when Bill 22 passed. Others came into force at a later date by regulation, some as recently as February 2023. The evolution of the law is also not confined exclusively to legislative amendments. Decisions of the Office of the Information & Privacy Commissioner ("OIPC") and the BC Courts also shape and interpret the understanding and application of FIPPA.

Two years on from these significant changes to FIPPA, we survey the differences to the FOI and privacy landscape in BC to see what has changed, what continues to evolve, and what remains to be seen. This paper outlines several regulatory changes that have come into force around privacy impact assessments, privacy management programs, application fees, and storage and disclosure of personal information outside of Canada. We also provide updates on recent OIPC decisions on section 43 of FIPPA, as expanded by Bill 22, as well as judicial review by the BC Supreme Court overturning OIPC decisions on disclosure of records.

II. THE NEW FIPPA LANDSCAPE – REGULATIONS UPDATES

A. Privacy Impact Assessment

A Privacy Impact Assessment ("PIA") is an internal assessment intended to evaluate any risks to personal information due to actions taken by a local public body. FIPPA itself does not provide much direction to local governments on conducting PIAs, providing only at section 69(5.3) that the "head of a public body that is not a ministry must conduct a privacy impact assessment and must do so in accordance with the directions of the minister responsible for this Act". Just a day after Bill 22 was passed, however, the Minister of Citizens' Services passed Ministerial Direction 2/21 – Directions to Heads of Public Bodies that are Not Ministries issued under Section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (the "PIA Directions"). The PIA Directions have had significant implications for when and how a PIA is conducted, clarifying that a public body must conduct a PIA "on a new initiative for which no PIA has previously been conducted" and, importantly, that a public body must also conduct a PIA "before implementing a significant change to an existing initiative, including but not limited to a change to the location in which sensitive personal information is stored, when it is stored outside of Canada."

The PIA Directions state that local public bodies are not required to use the provincial government's PIA template, but whatever format a PIA takes, it must assess a range of factors. Among other things, it must "identify privacy risks and privacy risk responses that are proportionate to the identified risk". Another requirement is to identify "reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made." If the initiative might involve storage outside Canada, a topic discussed in greater detail below, the public body must also assess whether the initiative "involves personal information that is sensitive" and whether it is to be "disclosed to be stored outside of Canada".

If the public body's initiative involves the use, collection, disclosure, or storage of personal information, the PIA must identify the privacy risks—the direction defines "privacy risk"—and identify "the level of the privacy risk(s) associated with the disclosure by examining factors", including risks such as the likelihood of unauthorized collection, the impact to individuals, whether the personal information is stored by a service provider, and where the personal information is stored. Public bodies must then, for each "privacy risk", identify a privacy risk response that is proportionate to the level of risk posed, including "technical, security, administrative or contractual measures". The overall outcome expected "will be a risk-based decision made by the head of the public body on whether to proceed with the initiative".

PIAs are generally for internal use only. However, there are times where a PIA must be submitted to the OIPC. As per section 69(5.4) of FIPPA, this is only statutorily required with respect to a proposed system, project, program or activity, if it addresses a "common or integrated program or activity", as defined in FIPPA. Any other PIAs can be submitted to the OIPC voluntarily for feedback, comments and suggestions, but there is no requirement to do so.

B. Privacy Management Programs

One of the last Bill 22 changes to take effect was the new requirements around privacy management programs ("PMPs"), which came into force on February 1, 2023. Under the new section 36.2 of FIPPA, all public bodies, including local governments, are required to develop a PMP in accordance with the provincial directive (the "Directive"),[1] also issued February 1st.

A PMP is a high-level holistic plan to manage privacy and security of personal information within the public body's custody or control. What a PMP looks like for a given public body may vary considerably depending on the scale of the organization and the volume and sensitivity of personal information that is dealt with. The Directive recognizes that "the amount or sensitivity

[1] *Privacy Management Program Direction*, February 1, 2023 <https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/pmp_ministerial_direction_2023.pdf>.

of personal information in the care of public bodies can vary substantially", and provides broad and scalable directions as to what a PMP requires. While this provides some flexibility for local governments in developing their PMPs, the Directive sets out some mandatory components that all public bodies must include in their PMPs.

As part of its PMP, a public body must designate a privacy officer. The privacy officer will be a point of contact for privacy-related matters, questions or concerns; support the development, implementation and maintenance of privacy polices; and support the public body's compliance with FIPPA. The privacy officer may be given additional roles and responsibilities, but these are the minimal duties required under the Directive.

Having clear and documented privacy procedures is also essential to any PMP. PMPs must include a process for completing and documenting PIAs and information-sharing agreements; a documented process for responding to privacy complaints and privacy breaches; and a process for regularly monitoring and updating the PMP itself to ensure ongoing compliance with FIPPA. Privacy policies, processes and practices must be made available to employees of the public body and, where practicable, to the public.

The Directive also requires the inclusion of educational and informative elements in PMPs. A public body must provide privacy awareness training and activities to ensure its employees are aware of their privacy obligations. A public body must also ensure that any service providers the public body works with are informed of their privacy obligations. This should be done both through awareness activities akin to those presented to employees, and through including clear and robust contractual terms addressing the service providers' privacy obligations.

For those local governments still developing their PMPs, or looking to further shore up and refine their existing PMP, the OIPC has developed a comprehensive guidance document[2] to assist public bodies in this area.

C. Application Fees

When the changes to FIPPA contained in Bill 22 were being considered and debated, one of the more contentious proposed changes was the addition of prescribed application fees – fees that would be charged to someone for making an access request. The debate around this point centred on whether an application fee would act as a barrier to access to information for some applicants; or conversely, if application fees might help reduce the strain on public bodies of high volumes of access requests and help offset costs associated with processing these requests. Opinions also varied as to what an appropriate amount for such a fee would be.

[2] *Accountable Privacy Management in BC'S Public Sector,* February 2023 <https://www.oipc.bc.ca/guidance-documents/1545>.

When Bill 22 was passed, the *Freedom of Information and Protection of Privacy Regulation* 155/2012 ("FIPPA Regulation") was also amended, with section 13(2) of the FIPPA Regulation setting the application fee at $10. This amount is in the lower range of fees charged in other jurisdictions, which range from $5 to $50. Under section 75(1)(a) of FIPPA, a public body can choose to charge the $10 application fee or not charge the fee, but cannot vary the fee amount. The application fee is distinct from and in addition to fees a public body has always been entitled to charge for work done fulfilling an access request (e.g., locating and retrieving records, providing copies of records), as per section 75(1)(b). An application fee may not be charged if the applicant is making a request for their own personal information, per section 75(3).

In January 2023, the OIPC published Investigation Report 23-01[3] which provided a review of the impact of application fees. The report compared access request data from analogous six-month periods between 2019 and 2022, before and after application fees went into place, as well as soliciting feedback from public bodies and applicants on their view of the effects of this change. The report focuses on the BC Provincial Government, but also surveyed 109 other public bodies, 24 of whom had opted to charge application fees, and 24 of whom were considering doing so in the future. The report states that overall, data does not indicate that the application fee was discouraging individual applicants from making general access requests. However, the report notes that certain categories of applicants, specifically media and journalists, have argued that the application fee poses a barrier. The OIPC also found that the data backed up the media's concern, indicating a decrease in both the total number of requests from media, and a decrease in the number of unique media applicants submitting requests.

The report also provides a number of recommendations to any public bodies that administer application fees, encouraging those public bodies to:

- Clearly inform applicants without delay when a fee applies;
- Ensure the time limit to respond to the access request is not suspended when they have failed to notify the applicant of the requirement to pay the fee;
- Have multiple fee payment options available to applicants, including an option that permits the applicant to maintain anonymity; and
- Establish a policy outlining the circumstances for when they will charge, or refund the fee.

[3] 2023 BCIPC 1 <https://www.oipc.bc.ca/investigation-reports/3744>.

Application fees under FIPPA have retained some of the controversy and discourse which surrounded them prior to Bill 22 coming into force – the Special Committee to Review FIPPA's report entitled "FIPPA for the Future" (the "Committee Report"),[4] for instance, notes ongoing concerns raised by such as the Canadian Association of Journalists and the Centre for Law and Democracy. However, the OIPC's report indicates that concerns over the application fee's deleterious effects on equal access to information have, at the present, not manifested to the degree some may have feared.

D. Storage and Disclosure of Personal Information Outside of Canada

Another major shift in the public sector privacy landscape put into motion by Bill 22 was the removal of the longstanding requirement that public bodies ensure that any personal information in their custody or control was stored and accessed solely in Canada. This data residency requirement, established by the former section 30.1 of FIPPA, severely limited public bodies' ability to utilize cloud technologies (e.g., cloud storage, videoconferencing, licenced software services), as employing most available services would necessitate hosting data outside of Canada.

Bill 22 repealed section 30.1 of FIPPA, removing the prohibition on storing or disclosing personal information outside of Canada. Public bodies are now allowed under FIPPA to store and disclose personal information in their custody or control outside of Canada, but must do so in accordance with the requirements of FIPPA and the *Personal Information Disclosure for Storage Outside of Canada Regulation*, B.C. Reg. 294/2021 ("Residency Regulation").

Under section 30 of FIPPA, a public body is obligated to implement reasonable security measures to protect information in its custody or control. This obligation applies to information inside and outside of Canada. The OIPC's guidance document on reasonable security measures for personal information disclosures outside of Canada[5] notes that when dealing with personal information outside of Canada, a very high level of rigour will be required in order to meet this duty to implement reasonable security measures.

Under the Residency Regulation, a PIA must be conducted for any program, project or system which involves "sensitive" personal information being stored outside of Canada. The Residency Regulation provides exceptions to this requirement, not requiring a PIA to be conducted for program project or systems in existence as of November 26, 2021, or for disclosure that is made to the general public as authorized or required by an enactment. While this may appear to indicate that PIAs are not required when non-sensitive personal information is being stored

[4] June 2022 <https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/3rd-session/fippa/report/SC-FIPPA-Report_42-3_2022-06-08.pdf>.
[5] March 2022 <https://www.oipc.bc.ca/guidance-documents/3646>.

outside of Canada, as discussed earlier PIAs are now a general requirement for new public body initiatives. Additionally, the dividing line between personal information that is or is not sensitive is not always clear.

The Residency Regulation refers to sensitive personal information, a term which is not defined in FIPPA or the Residency Regulation. While there is no fixed definition, some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used or disclosed. Types of information commonly accepted as "sensitive" include, but are not limited to, personal health information, personal financial information, criminal records, and information about sexual orientation, gender identity, religious or political beliefs, and race or ethnicity. Where outside of Canada the personal information is going to be stored is essential to determining whether that information might be "sensitive". Personal information that may not be considered sensitive in Canada may become sensitive when stored in another country with different political or legal realities.

III. CASELAW UPDATES

A. Systematic and Vexatious Requesters – Section 43

As a piece of legislation, FIPPA is fundamentally a balancing act, with the right of public access to information on one hand, and the right to privacy of information on the other. Another balance FIPPA seeks to strike is between the defence of access to information remaining equally open to all people, and providing some protections for public bodies against abusive or unreasonably burdensome use of FOI systems.

Under section 43 of FIPPA, public bodies may apply to the OIPC to disregard an access request if certain grounds apply. Prior to November 2021, the grounds to apply to disregard a request were twofold: where it can be demonstrated that the requests in question are frivolous or vexatious, or that the requests are repetitious or systematic to such an extent that fulfilling the requests would unreasonably interfere with the public body's operation. As part of the changes made by Bill 22, section 43 was expanded and now includes two further grounds to apply for authorization to disregard requests: where the request is for a record that has already been disclosed to the applicant, or is available to the applicant from another source, and where the request is so excessively broad in scope that it would unreasonably interfere with public body's operation. If the OIPC finds that section 43 applies, it can allow the public body to disregard all outstanding access requests from the applicant in question, or only allow the public body to disregard certain requests. The OIPC may also provide future relief under section 43, authorizing a public body to disregard future access requests from the applicant in question for a set period of time.

The OIPC approaches section 43 as an extraordinary remedy, which will only be granted in particularly dire circumstances. The OIPC acknowledges that section 43 is an important remedial tool which may curb abuse of the right to access, but also stresses that it must be used with great care and consideration, as it can limit or take away an individual's statutory right to access information.

Three recent decisions by the OIPC demonstrate the range of possible outcomes to section 43 submissions: refusal to authorize a public body to disregard requests; authorizing a public body to disregard current requests, but not authorizing them to disregard future requests from the same applicant; or authorizing a public body to disregard current and future requests for a set period of time.

1. Order F23-37 – TransLink

The South Coast British Columbia Transportation Authority (more commonly referred to as TransLink) applied to the OIPC per section 43 for authorization to disregard 18 outstanding access requests, and permission to disregard any future access requests (in excess of two requests per month) from the applicant for two years. The applicant had made access requests for videos and images of himself capture by TransLink CCTV systems on buses, skytrains, and transit stops. The 18 requests in question had been made over a period of six weeks, and the applicant had made 51 requests during the course of that year, and 62 requests the previous year. The applicant had a history of difficult interactions with bus drivers, and claimed to have been harassed by other passengers, and sought audio and video records of these interactions.

The Adjudicator considered the application of all grounds under section 43 to the applicant's requests. The Adjudicator found that the requests were not frivolous, as the applicant had a genuine interest in examining all audio and video recordings of himself. The Adjudicator also found the requests were not vexatious. Vexatious requests are requests made in bad faith, with an aim to harass, obstruct or pressure the public body in question, rather than having a genuine interest in the information being requested. TransLink argued that as the requests were not related to the purpose for which the CCTV system was implemented (to address violence, vandalism and other similar incidents on transit), they were made in bad faith, and that the volume of requests showed vexatious intent. The Adjudicator disagreed, holding that "abuse" under section 43 relates to abuse of a person's statutory right of access under FIPPA, not abuse of a records system's intended purpose. The Adjudicator also noted that a high volume of requests is not sufficient in of itself to indicate vexatious intent, noting that "[w]ithout more proof of an ulterior motive, the desire to view one's personal information out of genuine interest to know what a public body has collected about oneself does not make a request vexatious".

The Adjudicator also found that the requests were not an unreasonable interference on TransLink's operations. The requests in question were not found to be "repetitious" for the purpose of section 43. While the applicant had made numerous requests, he was not

requesting the same information in each request. Different requests specified different dates, buses and trains that the applicant sought records from. The requests were also not systematic. TransLink cited the increasing volume and frequency of the requests as evidence of their systematic nature. The Adjudicator held that although volume and frequency were important indicators of a systematic pattern of requests, they are not necessarily sufficient indicators on their own. Without something more to prove an intentional pattern to the applicant's behaviour, the Adjudicator stated that "in the absence of a clear motive, mode, plan or pattern, the volume and frequency of these requests alone do not meet the threshold for a finding that they are systematic … to be systematic, there must be a system involved". TransLink did not raise the broadness of the requests as causing unreasonable interference, so the Adjudicator did not consider this ground.

2. Order F22-61 – City of New Westminster

The City of New Westminster applied to the OIPC for relief under section 43(a), seeking authorization to disregard nine outstanding requests by an applicant (three of which were made during the course of the City's section 43 application) for being frivolous or vexatious. The City also sought future relief to disregard future access requests (in excess of one open request at a time). The applicant was a journalist seeking information about the circumstances of the City's former fire chief's retirement. The applicant made 16 requests between March and July of 2022, all of which were responded to by the City. The applicant sought an OIPC review of four of the City's responses, and was highly argumentative and accusatory in his communications with the City over the City's handling of his requests. In response to a letter from the City requesting the respondent be considerate and respectful of staff in his communications, the applicant filed the six further requests which lead to the City's section 43 application.

The Adjudicator granted the City authority to disregard the nine outstanding access requests, finding that the requests were vexatious under section 43(a). In finding the applicant's requests were vexatious, the Adjudicator weighed a number of non-exhaustive factors considered in previous OIPC decisions. The Adjudicator found that four of these factors in particular indicated that the applicant had an ulterior motive in making his requests: the type of information the applicant was requesting; the timing of the applicant's requests; the repetitiveness of the requests; and an absence of a genuine interest by the applicant in the records. The type of information the applicant requested targeted people within the City who had either refused to answer the applicant's questions, such as the Mayor, or people who disagreed with the applicant's accusations towards the City's fulfillment of its obligations under FIPPA, such as the City's Solicitor and Manager of Legal Services. The timing of the requests indicated a retaliatory intent from the applicant: six of the requests were made after the applicant received a letter from the City, and the remaining three were made after he received notice of the City's section 43 application. The Adjudicator also noted the repetitive nature of the requests, with subject matter repeated between requests. Finally, the Adjudicator noted the disconnect between the applicant's stated purpose in making the requests (obtaining information related to the former fire chief's retirement) and the actual access requests, which did not pertain to this subject.

Although the Adjudicator found that the applicant's nine outstanding requests were vexatious, they declined to offer the future relief sought by the City. The Adjudicator stated that authorizing the City to disregard future access requests "would be a wholly disproportionate remedy when it is not known whether any of the respondent's future requests would be vexatious", finding that there was insufficient evidence to indicate the applicant's future requests would also be vexatious.

3. Order F23-61 – Ministry of Attorney General

The Ministry of the Attorney General (the "Ministry") applied for authorization to disregard an applicant's outstanding access request, as well as certain future access requests by the applicant. The Ministry argued that the outstanding request was vexatious, per subsection 43(a), and systematic to the point of unreasonable interference with the Ministry's operations, per subsection 43(c)(ii). The applicant was a medical practitioner who had been engaged in a lengthy dispute with the Province over its audit of the applicant's MSP billings. Between 2017 and 2023 the applicant made 110 access requests to the Province and the Medical Services Commission. The Commission and the Ministry of Health had previously made a successful section 43 application to disregard requests by this applicant. The Ministry had previously made a section 43 application in 2021, and while the OIPC found the applicant's requests were systematic, it was not satisfied that the outstanding request would unreasonably interfere with the Ministry's operations.

The Adjudicator found that the applicant's outstanding request was vexatious and systematic, and that responding to it would unreasonably interfere with the Ministry's operations. The Adjudicator held that the applicant's own response submission indicated the improper purpose of his access request. The applicant's submissions repeated irrelevant and unsubstantiated arguments which the OIPC had dismissed in other orders in relation to the applicant. The applicant's submissions also devoted extensive time to berating the Ministry's lawyers. The Adjudicator found that the language in the applicant's response submission indicated "that the outstanding request was made, at least in part, for the purpose of proceeding to inquiry and harassing Ministry employees" and was part of the applicant's ongoing abuse of FIPPA.

The Adjudicator also found that the applicant's request was systematic in light of his history of access requests, complaints to the OIPC, and a previous order from the OIPC indicating that the respondent was systematically requesting records from the ministry. The Adjudicator also found that, given the broad scope and lengthy time period covered by the applicant's request, fulfilling it would unreasonably interfere with the Ministry's operations. The Ministry provided evidence indicating that fulfilling the request would likely require 1,160 hours of response time and generate 16,200 pages of responsive records.

The OIPC authorized the Ministry to disregard the outstanding record. The OIPC also granted future relief, authorizing the Ministry to limit the applicant to one open access request at a time for a period of five years.

B. Judicial Reviews

When the BC Supreme Court judicially reviews a decision made by the OIPC, the presumptive standard of review is reasonableness. The Court is tasked to consider the justification, transparency, and intelligibility of a decision, and whether it is justified in relation to the applicable facts and law. In reviewing a decision for reasonableness, the Court should have regard to both the outcome and the decision-maker's reasoning process. With that said, no deference is owed to an administrative decision-maker with respect to an allegation of procedural unfairness. The duty of procedural fairness is triggered whenever an administrative body's decision affects the rights, privileges, or interests of an individual. The content of this duty is inherently contextual and must be determined having regard to the circumstances of a given case.

1. *Burnaby (City) v. British Columbia (Information and Privacy Commissioner)*, 2023 BCSC 948

In *Burnaby (City) v. British Columbia (Information and Privacy Commissioner),* 2023 BCSC 948, the City of Burnaby successfully applied for judicial review of an OIPC Adjudicator's decision to compel production of certain redacted information. The access request was for "a list of all properties owned by [the City] in Burnaby and any properties that it may own in the province of B.C. Canada." The City responded with a 66-page spreadsheet that included many rows outlining a municipal address and/or property identifier ("PID") for a number of properties owned by the City. In 421 rows, however, the municipal addressees and/or PIDs were redacted (the "Redacted Properties") as that information related to the City's plans for future development projects. The Redacted Properties related to properties that were the subject of land acquisition projects where the City had targeted adjacent or proximate properties for acquisition and land assembly. The Redacted Properties were withheld by the City under section 17 of FIPPA, which provides that a public body can refuse to disclose information which, if disclosed, could "reasonably be expected to harm [its] financial or economic interests". Under s. 57(1) of FIPPA, the City had the burden of proving that the applicant had no right of access to the information withheld under s. 17(1).

At Inquiry, the Adjudicator concluded that the City had not met its burden of proof to establish that s. 17(1) applies to the information in dispute, and ordered the City to give the applicant access to the Redacted Properties (the "OIPC Decision"). The order was then stayed pending judicial review.

On judicial review, the City again took the position that if the Redacted Properties were released, it was a reasonable expectation that the City would suffer economic, financial, and other harms, as well as harm to its ability to negotiate the purchase of the targeted properties at fair market value. This was given the City's past experiences when land assembly goals became known to a property owner. It said that if the Redacted Properties were disclosed, it could be discerned from the groupings of the properties that properties adjacent or in close proximity to them are likely to be targeted or identified for land acquisition by the City.

The OIPC submitted that the OIPC Decision was grounded in the finding that the City had not established any "direct link" between those stated concerns and the Redacted Properties. The Adjudicator had held that many property owners may refuse to sell, or sell only at inflated prices, simply because the City has expressed an interest in their properties. The Adjudicator said a property owner may take such a position "regardless of when the property owner learns of the City's interest in their property", and that the risk of property owners seeking higher prices is "inevitable".

The City said that the Adjudicator focused on advance knowledge of the City's interest, rather than the impact of knowledge, not just of the City's interest, but of the purpose for which it sought to acquire the property, i.e., as part of an active land assembly package for future development or parkland. Finally, the City argued that disclosure of the Redacted Properties would provide owners of adjacent or proximate lands with a "virtual roadmap" in that anyone can then determine, with a high degree of certainty, where a land assembly is planned, and they could then determine how critical the purchase of their property is to the land assembly package so as to provide leverage for negotiating purposes.

The Court ultimately agreed with the City, finding that the Adjudicator misapprehended the City's evidence and the import of that evidence, and held that the OIPC Decision was unreasonable and should be set aside. The Court held that the Adjudicator erred in focusing on the timing issues, and, contrary to the Adjudicator's discussion in the OIPC Decision, the critical point of the evidence was that a property owner would then not only know that the City was interested in purchasing their property, but also have evidence about the City's likely assembly plans for their property and other properties, and how far along the City had progressed in its land acquisition toward that goal. The Court said that if a property owner becomes armed with that knowledge, the City's evidence established that there was considerably more risk that a property owner may ask for an increased sale price or refuse to sell at all, and, additionally, "the 'disclosure to the world' would also inevitably increase the risk of other third parties entering the fray to purchase the remaining properties in the yet uncompleted land assembly, seeking to acquire 'leverage' in relation to the City as a means for profit" (at para 53). Essentially, the Adjudicator failed to consider what the impact of disclosure of the Redacted Properties would be if property owners had that specific knowledge as well as knowledge of the City's plans and intentions with respect to the property.

The Court found that the City was only required to show that there was a "reasonable basis for believing that harm will result" from the disclosure that went beyond speculation or conjecture, not that harm would result or even was probable. As such, the Court found that the evidence provided by the City was not speculative and did meet the requirement of proving a reasonable expectation of probable harm, as required under s. 17(1) of FIPPA.

2. *Airbnb Ireland UC v. Vancouver (City)*, 2023 BCSC 1137

In *Airbnb Ireland UC v. Vancouver (City)*, 2023 BCSC 1137**,** Airbnb Ireland UC ("Airbnb") similarly applied for judicial review of an OIPC decision in relation to records held by the City of Vancouver about short-term rental accommodations. The City received access requests to disclose information that Airbnb had provided it pursuant to a memorandum of understanding (the "MOU"). The applicant sought Airbnb hosts' names, licence numbers and addresses, as well as information in relation to all short-term rentals in the City in addition to those on the Airbnb platform. The City refused the requests on the basis of sections 15 and 19 of FIPPA, which permit a public body to refuse to disclose information that could reasonably be expected to threaten an individual's safety or mental or physical health, or harm the security of the property. The City also relied on sections 21 and 22, which require a public body to withhold information if its disclosure could reasonably be expected to harm the business interests of a third party or involves personal information, the release of which would unreasonably invade a person's privacy.

At Inquiry, the OIPC rejected the City's arguments and ordered it to disclose: a) licence numbers of individuals on the Airbnb platform; b) home addresses of all Airbnb hosts in the City; and, c) the licence numbers associated with those addresses (the "Records").

Airbnb argued that the OIPC's decision was unreasonable and the result of an unfair process for three reasons:

- The OIPC's determination that the Records are not subject to sections 15 and 19 of FIPPA was unreasonable because it misapplied the provisions by requiring Airbnb and the City to demonstrate a greater risk of harm than is legally necessary;

- The OIPC's determination that the Records are not subject to section 22 was unreasonable because it would require Airbnb hosts to disclose the address of their principal residence, which together with the short-term rental licence numbers and other publicly available information could be used to identify Airbnb hosts; and

- The OIPC breached its duty of procedural fairness by failing to provide the Airbnb hosts with notice of the requests and an opportunity to participate in the hearing.

On issue one, the standard of proof applicable to sections 15 and 19 of FIPPA is the "reasonable expectation of probable harm". Both Airbnb and the City asserted that the OIPC correctly articulated the standard of proof applicable to the sections, but that it applied a higher threshold by requiring evidence of actual risk. They pointed to the OIPC's acceptance of the evidence provided by a stalking victim as support for their position. The OIPC found in that case that sections 15 and 19 were engaged in respect of that individual based on their past experiences and the risks to that individual if the Records relating to them were disclosed.

Airbnb and the City submitted that the OIPC's analysis of Twitter posts and media articles rose to the level of requiring probable harm by necessitating evidence akin to that provided by the stalking victim of an actual risk of harm. They said that the OIPC effectively required evidence from each Airbnb host whose personal information is contained in the Records, but failed to provide them with an opportunity to do so and instead ordered the release of their information. The City submitted that the evidence of the stalking victim was not only evidence of probable harm to that individual, but also evidence of a type of harm that could affect other Airbnb hosts if the Records were disclosed.

The OIPC argued that Airbnb and the City had not drawn any links between protest activities in other cities and harm to the life, safety or physical or mental health of anyone. The OIPC found that the suggestion that robbery or vandalism would be likely to occur if the Records were released did not rise above the level of mere possibility or speculation and that protests do not constitute harm to the security of a property or building.

The Court held that the OIPC had properly reviewed and considered the relevant evidence in respect of sections 15 and 19 in concluding that they did not apply. It did not require evidence of actual harm and, instead, sought a middle ground between mere possibility and probability. The Court found that the OIPC's reasoning process it applied in determining that the evidence did not meet the middle ground standard was clear, intelligible and reasonable, and that the decision was therefore entitled to deference. The Court accepted, however, that the stalking victim's evidence suggested that the risk to other Airbnb hosts' physical and mental well being could go beyond the individual's particular circumstances, which raised the prospect of other such evidence that may be important, discussed further on issue three.

With respect to issue two, Airbnb and the City asserted that the OIPC misinterpreted section 22 of FIPPA by finding that a home address was not personal information. The City's short-term rental bylaws compelled Airbnb hosts to provide their home addresses, which had factored into the OIPC's decision. The Court held that the OIPC's failure to consider the context in which the Airbnb hosts' principal residence addresses were required to be disclosed, and the finding that this information somehow lost its character as personal information merely because its disclosure was required, were not reasonable. The Court said that, "[t]aken cumulatively, it would enable the discovery of a treasure trove of personal information, the disclosure of which would completely distort the balance that FIPPA seeks to strike in section 2 between making public bodies more accountable to the public and protecting personal privacy" (at para 69).

Finally, on the third issue, the Court held that the OIPC had a duty to provide notice to all Airbnb hosts and an opportunity to participate in the Inquiry. This is because the "person most likely to be affected by the disclosure of a record is best placed to explain the impact of its disclosure" (at para 79). As this was in regards to procedural fairness, it was not subject to a reasonableness review, and the OIPC was not owed any deference on this portion of its decision.

The OIPC's decision was ultimately quashed and the matter remitted back to it for reconsideration based on the Court's reasons and after proper notice of the request was provided to the Airbnb hosts.

IV. CONCLUSION

While we are now a couple of years out from the last major legislative shift, our FOI and privacy laws are ever-changing and adapting. Decisions of the OIPC and the Courts, along with the recent regulatory changes we have outlined, continue to provide clarity on key areas of change. We await decisions on other newly introduced sections, such as section 3(5), the exclusion of the right to access certain forms of information, and section 18.1, the new mandatory exception for disclosure where the disclosure is harmful to the interest of Indigenous people. Stay tuned!

NOTES

NOTES