IN THE SUPREME COURT OF BRITISH COLUMBIA

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

Date: 20230704
Docket: S220590
Registry: Vancouver

Between:

Airbnb Ireland UC

Petitioner

And

The City of Vancouver,
The Office of the Information and Privacy Commissioner for British Columbia,
The Attorney General of British Columbia and
John Doe Requester

Respondents

Before: The Honourable Justice Basran

Reasons for Judgment

Counsel for the Petitioner:	M. Reynolds C. Hunter
Counsel for the Respondent, The City of Vancouver:	A. Aguilar
Counsel for the Respondent, The Office of the Information and Privacy Commissioner for British Columbia	K. Phipps
Place and Dates of Hearing:	Vancouver, B.C. January 18–19, 2023
Place and Date of Judgment:	Vancouver, B.C. July 4, 2023

Table of Contents

Introduction

[1] The petitioner, Airbnb Ireland UC ("Airbnb"), applies for judicial review of a decision of the respondent, the Office of the Information and Privacy Commissioner for British Columbia (the "IPC"), involving records held by the respondent, City of Vancouver (the "City"), regarding short-term rental accommodations ("STR"). The application raises questions regarding the release of information provided by individuals ("Hosts") who provide STR.

[2] The City received requests to disclose information Airbnb provided to the City pursuant to a memorandum of understanding (the "MOU") they entered. The requester (the "Requester") sought the Hosts' names, licence numbers, and addresses, as well as information in relation to all STRs in the City in addition to those on the Airbnb platform.

[3] The City refused the requests based on ss. 15 and 19 of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996 c. 165 [*FIPPA* or the *Act*]. These sections 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 ss. 21 and 22 of *FIPPA* 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.

[4] The IPC overturned the City's decision and ordered it to disclose:

a) licence numbers of individuals on the Airbnb platform;

b) home addresses of all Hosts in the City; and

c) the licence numbers associated with those addresses.

(the "Records")

[5] The relevant IPC order is Order F21-65 (the "Decision").

[6] Airbnb asserts that the Decision is unreasonable and the result of an unfair process for three reasons:

1) IPC's determination that the Records are not subject to ss. 15 and 19 of the *Act* is unreasonable because it misapplied these provisions by requiring Airbnb and the City to demonstrate a greater risk of harm than is legally necessary;

2) The IPC's determination that the Records are not subject to s. 22 is unreasonable because it will require Hosts to disclose the address of their principal residence. These addresses together with STR licence numbers and other publicly available information can be used to identify Hosts; and

3) The IPC breached its duty of procedural fairness by failing to provide Hosts with notice of the requests and an opportunity to participate in the hearing.

[7] Airbnb and the City seek an order quashing the Decision and confirming the City's decision not to release the Records. Alternatively, they seek an order that the matter be remitted back to the IPC with proper notice to the Hosts.

Factual Background

[8] Airbnb Ireland UC is a company established under the laws of the Republic of Ireland. It operates an online peer-to-peer marketplace for users residing outside of the United States and China to directly connect with each other. Travellers ("Guests") connect with Hosts to book services that Hosts advertise on this site, including STR accommodations.

[9] The City is a municipality in the Province of British Columbia. It is a public body for the purposes of the *Act*.

[10] In April 2018, the City amended its bylaws relating to STRs. Under these bylaws, a person who provides accommodation for less than 30 days at a time and in a dwelling unit other than a hotel or bed-and-breakfast, is deemed to be an STR operator and must obtain a licence from the City (the "STR Licence"). An individual is only allowed to operate a STR in their principal residence. Corporations and societies are not permitted to be Hosts. For this reason, Hosts are always

individuals and the STR Licence is issued to them in their own names and the address on the STR Licence are their home addresses.

[11] On April 10, 2018, the City and Airbnb entered the MOU, whereby Airbnb agreed to require that Hosts who wish to list a new STR in Vancouver obtain a STR Licence number as a prerequisite. Airbnb and the City also agreed that the City would receive information from Airbnb about the City's active listings, including Airbnb Hosts' names, their STR Licence numbers, home addresses, and email addresses, which the City can use to administer and enforce its bylaws. Pursuant to s. 1.9 of the MOU, the City confirmed that information disclosed by Airbnb was "Personal Information" under *FIPPA*.

[12] The City publicly discloses information on its Open Data Portal about the STR Licences issued, such as the status of the licence and whether the applicable fee has been paid. However, it does not post STR Hosts' names or STR addresses. Each STR Licence associated with a STR address can be linked to an identifiable individual using other publicly available information: Decision at para. 124.

[13] In 2018, the City stopped disclosing the names of STR Licence holders and addresses for home-based businesses on its Open Data Portal. It also deleted these addresses from its historical records. It took this step based on several credible reports of safety risks related the disclosure of residential addresses.

[14] While Hosts allow Guests to attend at their principal residence, they exercise a significant amount of control over disclosure of this address. This is because Hosts only communicate with Guests online through Airbnb or another STR platform and often only use a first name or pseudonym. The general area of the STR is described on the STR platform but not its exact location. Hosts vet each potential booking and can reject potential bookings if they have any concerns. Hosts are only required to disclose their home address after they have accepted a booking.

[15] In March 2019, the Requester made two separate requests for information from the City. The first was for information that Airbnb shared with the City between

November 1, 2018 and March 15, 2019, specifically, Airbnb Hosts' names, their STR Licence numbers, and their STR addresses. The second request is for information relating to the STR addresses and the STR Licence numbers of all STRs, not just Airbnbs, listed on the City's Open Data Portal during the same period. The City treated the two separate requests as one request (the "Request").

[16] This information is contained in two Excel files referred to in the Decision as Spreadsheet A and Spreadsheet B. Spreadsheet A contains the information responding to the first request (Airbnb Hosts' names, their STR Licence numbers, and their STR addresses). Spreadsheet B contains the information responding to the second request (all STR Hosts' addresses and their STR Licence numbers).

[17] The Request covers information about a large number of Hosts accounting for almost 20,000 total entries.

[18] In June 2019, the City refused the Request based on ss. 15(1)(f) and (l), 19(1)(a), 21, and 22 of the *Act*.

Legislative Framework

[19] The purposes of the *Act* are to make public bodies more accountable to the public and to protect personal privacy: s. 2 of *FIPPA*.

[20] Section 15 of the *Act* permits a public body to refuse to disclose information where the disclosure could reasonably be expected, *inter alia*, to endanger the physical safety of a person or harm the security of property:

> Disclosure harmful to law enforcement
>
> 15 (1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
>
> […]
>
> (f) endanger the life or physical safety of a law enforcement officer or any other person,
>
> […]
>
> (l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[21] Similarly, s. 19 permits the public body to refuse to disclose information where the disclosure could reasonably be expected to threaten a person's safety or mental or physical health:

> Disclosure harmful to individual or public safety
>
> 19 (1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, if the disclosure could reasonably be expected to
>
> (a) threaten anyone else's safety or mental or physical health, or
>
> (b) interfere with public safety.
>
> […]

[22] Section 21 requires a public body to refuse to disclose information that would be harmful to business interests of a third party.

[23] Section 22 requires a public body to refuse to disclose information that would be harmful to personal privacy:

> Disclosure harmful to personal privacy
>
> 22 (1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.
>
> […]

[24] Sections 21 and 22 of the *Act* are subject to the notice regime in s. 23. If a public body intends to give access to a record and there is reason to believe it contains information that might be excepted from disclosure under certain sections of the *Act*, it must give the third party written notice advising them of the request, the contents of the record, and an opportunity to make representations on whether the information should not be disclosed.

[25] If, after giving notice to the third party under s. 23, the public body decides to order the disclosure of the record at issue, pursuant to s. 24, the public body must notify the third-party of that decision. The third party may then seek review of the decision before the requester is granted access to the record.

[26] In this case, the City decided not to give access to the Hosts' information contained in the Records. It was therefore not required to give affected Hosts notice of the Request.

The IPC Appeal

[27] The Requester appealed the City's decision to the IPC.

[28] The City filed an affidavit from Kathryn Holm, the City's Chief Licence Inspector and Director of Licensing and Community Standards (the "Holm Affidavit"), and affidavits from Barbara Van Fraassen, the City's Director of Access to Information and Privacy (the "Van Fraassen Affidavits").

[29] The Holm Affidavit provides details of the privacy implications on Hosts if the Records are disclosed:

> While the Airbnb and Business Licence Information only consists of names and addresses, this information is highly sensitive as it identifies STR Operators' principal residence and, along with the business licence number, can be used to connect significant additional information about individual operators from STR listings.
>
> STR listings regularly contain significant amounts of personal information, either directly or through reviews left by past guests. Further personal information may be disclosed in an STR listing by an owner about a tenant or vice versa without the consent of the other party as the City permits both owners and tenants to apply for STR business licences.
>
> Disclosure of the Airbnb and Business Licence Information would allow any reasonably informed person to link the information in these datasets with a specific STR listing. This would connect the STR listing to the name and address of the STR Operator in the case of the Airbnb Information and the STR Operator's principal residence in the case of the Business Licence Information.
>
> One key piece of personal information from STR listings is availability… Disclosure of when a primary residence is available both discloses personal information about a person's travel patterns and increases the risk of criminal activity such as vandalism or robbery as bad actors could identify when the property is unlikely to be occupied.

[30] The Holm Affidavit also describes the risks to Hosts and Guests of disclosing the Records. Ms. Holm deposed that:

> People in Vancouver have diverse and often strong views on STR […] While much of the debate is healthy, several individuals opposed to STR have engaged in vigilante activities identifying STR Operators and harassing them online and in person. This concerted vigilante activity is particularly problematic as those involved seek to "name and shame" subject STR Operators and expose these individuals to threats, ridicule, and derision without any type of investigation as to the truth of the allegations.

[31] Ms. Holm described obscene, aggressive, and threatening Twitter posts directed at STR Operators and detailed reports of STR Operators being confronted by those opposed to STR activities. In light of this, Ms. Holm deposed that:

> STR Operators are the only group of business licence holders that have been subject to this level of harassment […] Public disclosure of the name and address of STR Operators will allow adversarial parties to independently verify suspicions and use this information to continue their harassment […] Disclosure of this information, particularly in conjunction with STR listing information, would harm the security of residences used for STR as it would provide details of likely occupancy, contents of suites, and access points, that would enable or encourage criminal activities such as vandalism and robbery.

[32] The Van Fraassen Affidavits describe the City's deliberate decision in 2018 to no longer disclose addresses for home-based businesses and to delete those addresses from historical records on the City's Open Data Portal following "several credible reports of safety risks related to the disclosure of residential addresses".

[33] Ms. Van Fraassen also described one particular episode in April 2019, in which a stalking victim contacted the City and advised that their stalker had previously used online databases to determine the person's whereabouts and that disclosing their name or even the city in which they lived could pose a real danger to their health and safety.

[34] Airbnb submitted an affidavit from Nathan Rothman, a Senior Campaign Manager, in which he deposed that "in Vancouver, Airbnb opponents have publicly urged others to occupy and refuse to leave Airbnb units" and "Airbnb opponents have also been engaged in attempts to publicly identify and harass Hosts in Vancouver online, in particular on Twitter".

[35] Hosts did not receive notice of the Request so the IPC did not have any representations or evidence from any person whose personal information would be disclosed through the release of the Records.

The IPC's Decision

[36] In its Decision, the IPC acknowledged that ordering the release of the Records to the Requester would mean disclosure to the world, given the likelihood that the Requester would share them broadly, and because the *Act* places no restriction on what a requester can do with disclosed information.

[37] With respect to ss. 15(1)(f) and 19(1)(a) of the *FIPPA*, the IPC concluded that, with the exception of the stalking victim who had contacted the City and requested that their information not be disclosed, the City and Airbnb had not shown a reasonable expectation that releasing the Records could threaten anyone's life, physical safety, and physical or mental health.

[38] On s. 15(1)(l), the IPC found that the City and Airbnb had not shown a reasonable expectation that the release of the Records could result in harm to property.

[39] With respect to s. 21, the IPC held that the names and addresses of Hosts (set out in Spreadsheet A) engaged s. 21(1)(a) and the City was therefore required not to disclose them. The IPC further held that the Airbnb STR Licence numbers in Spreadsheet A were not subject to the exception in s. 21 because disclosing that information could not reasonably be expected to cause harm.

[40] The IPC held that Hosts' addresses were provided to the City to receive a STR Licence and are therefore "business information" and not "personal information". For that reason, this information did not engage the exception in s. 22.

[41] The IPC further held that while STR Licence numbers were "personal information", their release was permitted pursuant to s. 22(4)(i) of the *Act*, which provides that a disclosure of personal information is not an unreasonable invasion of

a third party's privacy in the case of a licence, permit, or any other similar discretionary benefit.

Issues

[42] This application raises four issues:

a) What is the applicable standard of review?

b) Was it reasonable for the IPC to determine that releasing the Records could not reasonably be expected to endanger the physical safety, harm the security of any property, or threaten the mental or physical health of Hosts, pursuant to ss. 15 and 19 of the *Act*?

c) Was it reasonable for the IPC to determine that releasing the Records would not involve disclosure of personal information that would be an unreasonable invasion of a third party's personal privacy, pursuant to s. 22?

d) Did the IPC breach its duty of procedural fairness by not notifying Hosts of the Request?

[43] The IPC sought and was granted an expanded role at the hearing of this matter because there is no other petition respondent making arguments in support of the merits of the Decision.

a) The applicable standard of review

[44] Reasonableness is the standard of review applicable to the IPC's analysis of ss. 15, 19, and 22.

[45] The Court should 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*: Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65 at paras. 82–87 [*Vavilov*].

[46] No deference is owed to an administrative decision-maker with respect to an allegation of procedural unfairness: *Murray Purcha & Son Ltd. v. Barriere (District)*, 2019 BCCA 4 at para. 28.

b) Was the IPC's determination reasonable that releasing the Records could not reasonably be expected to endanger the physical safety, harm the security of any property, or threaten the mental or physical health of Hosts?

Relevant legal principles

[47] The standard of proof applicable to ss. 15 and 19 is the "reasonable expectation of probable harm". This requires showing more than a mere possibility of harm but it does not require evidence of a risk of harm on a balance of probabilities: *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3 at para. 197 [*Merck Frosst*].

[48] This standard was summarized in *British Columbia Hydro and Power Authority v. British Columbia (Information and Privacy Commissioner)*, 2019 BCSC 2128:

> [85] The burden rests with BC Hydro to establish that the disclosure of the employees' names could result in a reasonable expectation of probable harm: *FIPPA*, s. 57; *Merck Frosst* at para. 195. The test is summarized in [*Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 [*Community Safety*]]:
>
> > [54] This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground: paras. 197 and 199. This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations or consequences": *Merck Frosst*, at para. 94, citing *F.H. v. McDougall*, 2008 SCC 53, [2008] 3 S.C.R. 41, at para. 40.
>
> [86] This test is intended to balance the goal of disclosure against the need to avoid harm to third parties resulting from disclosure: *Merck Frosst* at para. 204. A succinct description of what is meant by a "reasonable expectation of probable harm" was articulated by Justice Cromwell, as he then was, at para. 196 of *Merck Frosst*: "[W]hile the third party need not show on a balance of probabilities that the harm will in fact come to pass if the records are disclosed, the third party must nonetheless do more than show that such harm is simply possible."

> [87] In addition to the Supreme Court of Canada jurisprudence, this Court has provided guidance on this point: *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner)*, 2012 BCSC 875. More recently, Justice Powers helpfully summarized this law in *United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada, Local 170 v. British Columbia (Information and Privacy Commissioner)*, 2018 BCSC 1080:
>
> > [42] Justice Cromwell indicated that the "reasonable expectation of probable harm" standard is intended to strike a balance between the important goals of disclosure on one hand, and avoiding harm to third parties resulting from disclosure on the other hand. To achieve this balance, the standard requires harm that is more than simply "fanciful, imaginary or contrived", but the standard does not go so far as requiring proof that the harm is more likely than not to occur (para. 204). In *Community Safety* at para. 59, Cromwell J. and Wagner J. (as he was then) noted that to meet the "reasonable expectation of probable harm" standard, there must only be a reasonable basis for believing that harm will result, and that the standard does not require a demonstration that harm is probable.
> >
> > [43] In *Community Safety*, the Court wrote that the "reasonable expectation of probable harm" standard should be used wherever the "could reasonably be expected to" language is used in access to information statues (para. 54). Section 21(1)(c) of the *FIPPA* uses the "could reasonably be expected to" language.
>
> [88] The courts have articulated a middle ground: to rely on s. 19(1)(a) of *FIPPA*, the public body does not need to prove the harm will *probably* occur if the information is disclosed. However, the mere *possibility* of harm is also not sufficient. Put another way, the test articulated by the Supreme Court of Canada is that the probability of the harm need only be reasonably expected; the test does not require probable or actual harm: *Community Safety* at para. 54

Positions of the parties

[49] Airbnb and the City assert that the IPC correctly articulated the standard of proof applicable to ss. 15 and 19 but that it applied a higher threshold by requiring evidence of actual risk. They point to the IPC's acceptance of the evidence provided by the stalking victim as support for their position. The IPC found that ss. 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.

[50] Airbnb and the City submit that the IPC'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 further assert that

it was incumbent on the IPC to notify Hosts of the Request so they could provide their submissions about the risks posed by releasing the Records. This is because the IPC effectively required evidence from each 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.

[51] The City submits 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 Hosts if the Records were disclosed.

[52] The IPC contends that it found that the Twitter posts did not threaten or express hostility towards individuals or allude to physically harming any person or building. Furthermore, the IPC argues 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 IPC found that the suggestion that robbery or vandalism would be likely to occur if the Records were released did not rise above the level or mere possibility or speculation and that protests do not constitute harm to the security of a property or building.

Discussion

[53] Sections 15 and 19 are harm-based exceptions to the right of access in the *Act*. Sections 15(1)(f) and 19(1)(a) involve harm to a person and s. 15(1)(l) concerns harm to property.

[54] I am satisfied that the IPC tried to carve out a middle ground between what is probable and merely possible. In assessing the Twitter posts and media articles, it considered if the evidence went “well beyond” or “considerably above” a mere possibility of harm to the life, safety or physical or mental health of the Hosts. It concluded that the evidence before it did not meet this standard.

[55] In assessing threats to mental health in s. 19(1)(a), the IPC determined that disclosure of the Records would not lead to more than usual upset, or risk serious mental distress or anguish approaching a clinical issue. I accept the IPC’s

demarcation of the standard in this manner as its attempt to find a middle ground that is well beyond and considerably above a mere possibility.

[56] In my view, the IPC properly reviewed and considered the relevant evidence in respect of ss. 15 and 19 in concluding that they did not apply. It did not require evdience of actual harm and, instead, sought a middle ground between mere possibility and probability. Its decision is justified in relation to the general and broad nature of the Twitter posts and media articles that it considered. The reasoning process it applied in determining that this evidence did not meet the middle ground standard is clear, intelligible, and reasonable. This decision is therefore entitled to deference.

[57] While I accept that the stalking victim's evidence may suggest that the risk to other Hosts' physical and mental well being may go beyond this individual's particular circumstances, this specific evidence when considered with the other relevant evidence of harm, does not meet the middle ground standard. It does, however, raise the prospect of other such evidence that may be important. As described later in these Reasons, I have concluded that the IPC is required to provide notice to the Hosts of the Request.

c) Was the IPC's determination reasonable that releasing the Records would not involve disclosure of personal information that would be an unreasonable invasion of a third party's personal privacy?

Relevant legal principles

[58] A public body must withhold personal information where disclosure would lead to an unreasonable invasion of a third party's personal privacy: s. 22 of the *Act*.

[59] Personal information is defined as "recorded information about an identifiable individual other than contact information": Schedule 1 of *FIPPA*.

[60] The IPC concluded that information is "about an identifiable individual" if it is reasonably capable of identifying that individual, either alone or in tandem with other available sources of information: Decision at para. 112.

[61] Contact information is defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual": Schedule 1 of *FIPPA*.

[62] Whether information is contact information in any given circumstance depends on its context: Decision at para. 113.

[63] Disclosing a third party's name, address, or telephone number for use on mailing lists or telephone solicitation is presumptively an unreasonable invasion of their personal privacy: s. 22(3)(j) of the *Act*.

Positions of the parties

[64] Airbnb and the City assert that the IPC misinterpreted s. 22 of the *Act* by finding that a home address was not personal information. The Hosts are required to provide their home address to the City because, unlike any other business, the City requires that all STRs be operated from a principal residence. Accordingly, the City's STR bylaws compel Hosts to provide their home addresses, and this is personal information.

[65] The City further submits that the IPC's reasoning is flawed because it found that disclosure of the information in the Records would allow a third party to obtain significant additional information contained in anonymized STR listings. However, it failed to consider the cumulative information disclosed in relation to all relevant issues, including whether names and principal residence addresses were exempt from protection of "personal information" because they fell within the definition of "contact information".

[66] The IPC asserts that it is an expert in its home statute, which includes the application of the facts before it to the definitions in the statute. Aside from the cumulative information argument, which was not advanced during the IPC appeal, the IPC considered the evidence and relevant arguments, applied the relevant legal

principles and made its determination. The IPC therefore submits that this suggests that the IPC made a reasonable decision to which deference is owed.

Discussion

[67] In my view, the IPC's failure to consider the context in which the Hosts' principal residence addresses were required to be disclosed was unreasonable. The finding that this information somehow loses its character as personal information merely because its disclosure is required in order to comply with the requirement to obtain a STR Licence is not reasonable.

[68] The Hosts' principal residence addresses are not binarily contact information or personal information. The context within which the disclosure of this information is required by the City must be properly considered and evaluated. The IPC understood that the Request sought the home addresses of the Hosts but nevertheless failed to do this contextual assessment and, instead, found that this information was contact information and therefore not entitled to protection from widespread disclosure.

[69] The IPC's finding that STR Licence numbers are personal information, but principal residence addresses are not, is confounding. The latter has a much closer connection to the personal lives and details of the Hosts. STR Licence numbers, Hosts' principal residence addresses, and the acknowledged ability of anyone to find the names of individual Hosts, in and of itself, constitutes the disclosure of a wide range of personal information. Taken cumulatively, it would enable the discovery of a treasure trove of personal information, the disclosure of which would completely distort the balance that the *Act* seeks to strike in s. 2 between making public bodies more accountable to the public and protecting personal privacy.

[70] I do not accept the IPC's rationale that by virtue of a principal residence being used as a place of business, this information loses its character as personal information. This binary analysis fails to consider the relevant context and risks of the disclosure of this information and is therefore unreasonable.

d) Did the IPC breach its duty of procedural fairness by not notifying Hosts of the Request?

Relevant legal principles

[71] The duty of procedural fairness is triggered whenever an administrative body's decision affects the rights, privileges, or interests of an individual: *Taseko Mines Limited v. Canada (Environment)*, 2019 FCA 320 at para. 28 [*Taseko*] citing *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 S.C.R. 817 at para. 20, 1999 CanLII 699.

[72] The content of this duty is inherently contextual and must be determined having regard to the circumstances of a given case: *Taseko* at para. 30 and *Baker* at para. 21.

[73] A non-exhaustive list of factors that inform the content of the duty of procedural unfairness includes:

a) The nature of the decision being made, and the process followed in making it;

b) The nature of the statutory scheme;

c) The importance of the decision to the affected individual or individuals;

d) The legitimate expectations of the person challenging the decision; and

e) The choices of procedure made by the administrative decision maker itself.

See *Baker* at paras. 23–27, cited with approval in *Vavilov* at para. 77.

[74] The purpose of the participatory rights contained within the duty of procedural fairness is to "ensure that administrative decisions are made using a fair and open procedure, appropriate to the decision being made and its statutory, institutional, and social context, with an opportunity for those affected by the decision to put forward their views and evidence fully and have them considered by the decision-maker": *Baker* at para. 22, cited with approval in *Taseko* at para. 29.

[75] Section 54 of the *FIPPA* provides:

> Notifying others of review
>
> 54 On receiving a request for a review, the commissioner must give a copy to
>
> (a) the head of the public body concerned, and
>
> (b) any other person that the commissioner considers appropriate.

[76] If the head of a public body intends to give access to a record that the head has reason to believe contains information that "might be" excepted from disclosure, the head "must" give notice to the third party and provide an opportunity to make submissions on why the information should not be disclosed: s. 23 of the *Act*.

Positions of the parties

[77] Airbnb and the City submit that the duty of procedural fairness required that the IPC notify Hosts of the Request and give them an opportunity to explain how disclosure of the Records would affect them and the IPC breached this duty by not providing this notice to the Hosts.

[78] The IPC notes that no participant asked the IPC to provide notice to Hosts pursuant to s. 54 and no Hosts attempted to intervene in this judicial review or contacted the IPC requesting that the matter be reopened to provide them with an opportunity to make submissions. The IPC also contends that the requirement to provide notice to the Hosts rested with the City, not the IPC, and providing notice would not have been easy because it would have required notice to individuals named in 20,000 entries.

Discussion

[79] The person most likely to be affected by the disclosure of a record is best placed to explain the impact of its disclosure. Hosts are inherently affected by the IPC's decision because it is their personal information and privacy interests at stake if the Records are disclosed.

[80] The IPC held that the City's evidence from the stalking victim, who proactively requested that the City not disclose their information, rose to the level of a reasonable expectation of probable harm. Similarly, serious, or analogous

submissions may have been provided by other Hosts had they been notified of the Request.

[81] I am satisfied that the IPC had reason to believe that the Hosts' information "might be" excepted from disclosure so they were under a duty to provide notice to all Hosts of the Request and an opportunity to participate, before making its decision on disclosure of the Records.

[82] This further information may well have met the standard of reasonable expectation of probable harm such that the IPC may have decided to withhold the disclosure of the Hosts' principal residence addresses either selectively or completely, depending on the nature and extent of the submissions received.

[83] I disagree with the IPC's contention that its decision not to notify Hosts, pursuant to s. 54 of the *Act*, is subject to a reasonableness review. In my view, the purpose of s. 54 is to ensure procedural fairness. This section is silent as to the rights of the parties who the IPC elects not to notify. For this reason, I am satisfied that the IPC is not owed any deference on its decision not to notify Hosts of the Request.

[84] Furthermore, the IPC did not provide reasons for its decision not to notify the Hosts so there is no way to meaningfully assess the justification, transparency, and intelligibility of this implicit decision.

Disposition

[85] The IPC's Decision is quashed, and the matter is remitted back to it for reconsideration based on these Reasons and after proper notice of the Request is provided to the Hosts.

Costs

[86] Airbnb will have its costs at Scale B from the IPC. There will be no order of costs for or against the City.

"Basran J."

No. VLC-S-S-■
Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

AIRBNB IRELAND UC

Petitioner

AND:

THE CITY OF VANCOUVER, THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, THE ATTORNEY GENERAL OF BRITISH COLUMBIA and JOHN DOE REQUESTER

Respondents

PETITION TO THE COURT

ON NOTICE TO:

The City of Vancouver, Vancouver City Hall, 453 12th Avenue, Vancouver, BC V5Y 1V4, **The Office of the Information and Privacy Commissioner for British Columbia**, 947 Fort Street, Victoria, BC V8V 3K3, the **Ministry of the Attorney General,** Deputy Attorney General, PO BOX 9280, Stn Prov Govt, Victoria, BC V8W 9J7, and **JOHN DOE REQUESTER**.

This proceeding is brought for the relief set out in Part 1 below by

☐ the person(s) named as petitioner(s) in the style of proceedings above.

☒ Airbnb Ireland UC (the petitioner)

If you intend to respond to this petition, you or your lawyer must

(a) file a Response to Petition in Form 67 in the above-named registry of this court within the time for Response to Petition described below, and

(b) serve on the petitioner

(i) 2 copies of the filed Response to Petition, and

(ii) 2 copies of each filed Affidavit on which you intend to rely at the hearing.

Orders, including orders granting the relief claimed, may be made against you, without any further notice to you, if you fail to file the Response to Petition within the time for response.

Time for Response to Petition

A Response to Petition must be filed and served on the petitioner,

(a) if you were served with the petition anywhere in Canada, within 21 days after that service,

(b) if you were served with the petition anywhere in the United States of America, within 35 days after that service,

(c) if you were served with the petition anywhere else, within 49 days after that service, or

(d) if the time for response has been set by order of the court, within that time.

(1) The address of the registry is:
Vancouver Registry
800 Smithe Street
Vancouver, BC V6Z 2E1

(2) The ADDRESS FOR SERVICE of the petitioners is:
c/o Molly Reynolds
Torys LLP
79 Wellington St. W., 30th Floor
Box 270, TD South Tower
Toronto, ON M5K 1N2
Fax number address for service (if any) of the petitioners:
416.865.7380
E-mail address for service (if any) of the petitioners:
mreynolds@torys.com

(3) The name and office address of the petitioners' lawyer is:
c/o Molly Reynolds
Torys LLP
79 Wellington St. W., 30th Floor
Box 270, TD South Tower
Toronto, ON M5K 1N2

CLAIM OF THE PETITIONER

Part 1: OVERVIEW & ORDER SOUGHT

1. This is an application for judicial review by Airbnb Ireland (UC) (**"Airbnb"**) of a decision of the Office of the Information and Privacy Commissioner (the **"IPC"**) concerning records relating to short term rental (**"STR"**) accommodation within the City of Vancouver (the **"City"**).

2. The IPC ordered the City to disclose (i) license numbers of individuals listing on the Airbnb platform, (ii) STR addresses held by the City more broadly (i.e. not just those relating to the Airbnb platform), and (iii) the license numbers associated with those addresses (the **"Records"**). The IPC's order is identified as Order F21-65 and referred to herein as the **"Decision"**.

3. The Decision is unreasonable in the following respects and as described further in this Petition:

   (a) The IPC erred in holding that the Records are not subject to Sections 15 and 19 of the *Freedom of Information and Protection of Privacy Act* (the **"*Act*"**),[1] which permit a public body to refuse to disclose information where disclosure could reasonably be expected to threaten an individual's safety or mental or physical health;

   (b) The IPC erred in holding that the Records are not subject to Section 22 of the *Act*, which requires the head of a public body to refuse to disclose personal information if the disclosure would be an unreasonable invasion of a third party's personal privacy; and

   (c) The IPC breached the duty of procedural fairness and the rules of natural justice by failing to provide notice of the request and the Decision to the Airbnb and other hosts associated with the requested addresses and license numbers, whose privacy interests and rights under the *Act* are at issue.

4. Accordingly, the Petitioner seeks the following relief:

   (a) An interlocutory Order directing the IPC to file the underlying record of proceedings;

   (b) An interlocutory Order staying the Decision and prohibiting the City from disclosing the Records until this application has been fully and finally decided;

[1] RSBC 1996, c 165

(c) An Order quashing the Decision and confirming the decision of the City of Vancouver as described herein;

(d) In the alternative, an Order quashing the Decision and remitting the matter back to the Commission for reconsideration on proper notice to all parties impacted by the Decision;

(e) Costs of the proceeding against any party who opposes the Petition; and

(f) Such further and other relief as to this Honourable Court may seem just.

Part 2: FACTUAL BASIS

Parties & Background

5. Airbnb is a company established under the laws of the Republic of Ireland. Its online platform connects individuals seeking short term accommodation (guests) with those offering it (hosts).

6. The City is a municipality in the Province of British Columbia incorporated in 1886 and a public body for the purposes of the *Act*.

7. The City first began regulating STRs in April 2018 through Bylaw 4450. Under that bylaw, a person who provides temporary accommodation in a dwelling unit other than a bed and breakfast or hotel is deemed an STR operator and required to obtain a licence from the City.

8. Only individuals are permitted to operate STRs in the City and an individual is only allowed to operate an STR in their principal residence (i.e. their own home and not in an investment property or secondary residence). As a result, all STR operators are individuals and licences are issued in the individual's own name and using their home address.

9. Most companies offering online STR platforms are registered outside of British Columbia and cannot be legally compelled by the City to operate within provincial and municipal rules. The City therefore attempts to engage and negotiate with them.

10. On April 10, 2018, the City and Airbnb entered into a Memorandum of Understanding (**"MOU"**), pursuant to which Airbnb agreed that its Vancouver hosts would need a City licence number to list on its online platform. Airbnb also agreed to provide information to the City about each Airbnb host's name, licence number, email address and STR address, which the City can use to regulate STRs via its bylaws.

11. The City publicly discloses information on its Open Data Portal about the licences it issues, including licences to operate STRs. However, given the safety and

privacy concerns, the City does not post STR operators' names, addresses or contact information.

The Request & the City's Decision

12. In March 2019, the Requestor made two separate access requests for information from the City. The first was for the information Airbnb shares with the City pursuant to the MOU, namely Airbnb hosts' names and the associated license numbers and addresses for their STRs during a five-month timeframe. The second was for the location information of all STRs listed on the City's Open Data Portal (i.e. not just Airbnbs') during the same period (collectively, the **"Requests"**).

13. In substance, the requested information consists of the following:

    (a) STR addresses, STR operators' names and the associated licence numbers in provided by Airbnb to the City; and

    (b) STR addresses and the associated licence numbers otherwise in the City's possession (i.e. not just relating to Airbnb).

14. The City declined to produce these records based on Sections 15(1)(f) and (l), 19(1)(a), 21(1) and 22(1) of the *Act*, which permit or require a public body not to disclose information where the information would:

    (a) reasonably be expected to endanger a person's life or physical safety (15(1)(f));

    (b) reasonably be expected to harm the security of any property (15(1)(l));

    (c) reasonably be expected to threaten a person's safety or mental or physical health (19(1)(a));

    (d) be harmful to the business interests of a third party (21(1)); or

    (e) be an unreasonable invasion of a third party's personal privacy (22(1)), respectively.

The IPC Appeal & Decision

15. The Requestor sought a review of the City's decision by the IPC.

16. Airbnb was granted leave to participate in the IPC proceeding, including to make submissions on the application of Sections 21(1) and 22(1) of the *Act*.

17. The City and Airbnb filed extensive submissions, including affidavit evidence, in support of the City's decision.

18. The IPC ordered the City to disclose the Records. More specifically, the IPC ordered as follows:

    (a) Sections 15(1)(f), 15(1)(l), 19(1)(a), 21(1) or 22(1) do not authorize the City to refuse access to the information in dispute, with the exception of records relating to one Airbnb host who is being stalked, in respect of whom the City is authorized by Sections 15(1)(f) and 19(1)(a) of the *Act* to refuse disclosure;

    (b) The City is required by section 21(1) of the *Act* to refuse to disclose the Airbnb hosts' names and the STR addresses (contained in Spreadsheet A); and

    (c) The City is otherwise required to provide the Requestor with access to all other information sought (i.e. the Records).

19. The IPC did not provide notice of the proceeding or the Decision to any STR operators or other third parties impacted by the Decision and no other third parties participated in the IPC proceeding aside from Airbnb.

Part 3: LEGAL BASIS

20. The Decision is unreasonable and should be quashed.

The IPC Misconstrued Sections 15 and 19 of the *Act*

21. The IPC erred in holding that the Records are not subject to Sections 15(1)(f),(1) and 19(1)(a) of the *Act*, which exempt information from being disclosed that gives rise to a reasonable expectation of probable harm to personal safety or property, including physical and mental health.

22. First, the IPC misapplied the legal test for determining whether disclosure of the Records engages a reasonable expectation of probable harm to personal safety or property.

23. As the IPC itself acknowledged, while the "reasonable expectation of probable harm" standard requires evidence going beyond a mere possibility of harm, it does not require proof even on a balance of probabilities.

24. In order to demonstrate the risks posed by the disclosure of the Records, Airbnb and the City submitted evidence of an Airbnb host who had previously reported to Airbnb that her stalker could locate her if her address and/or name were disclosed on the City's Open Data Portal.

25. The IPC found, correctly, that this demonstrated a reasonable expectation of probable harm and engaged the exemptions in Sections 15 and 19 of the *Act*.

26. However, the IPC held that these exemptions only applied in respect of the specific individual who had proactively reported her concerns to the City, and not to any other Airbnb host who had not volunteered evidence of specific harm.

27. In so holding, the IPC misapplied the legal test and required, in effect, actual proof of probable harm for each STR operator.

28. The IPC also erred in its application of Sections 15 and 19 by failing to give any consideration or have any regard to the different risks posed to vulnerable hosts including members of equity-seeking groups by its disclosure order.

29. Second, the IPC erred by failing to consider the extent to which online harassment and cyber-bullying could reasonably be expected to threaten individuals' mental health and thereby engage Sections 15 and 19.

30. The IPC correctly found that disclosure of the Records to the Requestor would be disclosure to the world, and that the *Act* places no restriction on what the Requestor can do with the information. The IPC acknowledged that the Requestor had posted numerous times on social media about STRs and that it is reasonable to expect that the Requestor will share the information disclosed in response to the Requests.

31. If the Decision is not quashed, the Requestor can be expected to publish the information broadly, and any number of individuals will be able to use the information to harass, threaten or abuse the STR operators, and locate or attend at their homes. Although the *Act* does not require the Requestor to establish their purpose for making an access request, the IPC erred in discounting the probability of harm to personal safety or property that may arise from broad publication of the Records.

32. Airbnb filed extensive evidence of social media and other online posts by the Requestor and others disparaging Airbnb hosts. Despite acknowledging that the posts reflect "inflammatory language such as "parasite", "bedbugs", "infestation" and the F-word to refer to STRs, Airbnb and Airbnb users generally", the IPC misconstrued the significance of this evidence by failing to consider the extent to which such online harassment and cyberbullying could itself ground a reasonable expectation of probable harm.

The IPC Misconstrued Section 22 of the *Act*

33. The IPC erred in holding that the Records are not subject to Section 22 of the *Act*, which requires public bodies not to disclose personal information if the disclosure would be an unreasonable invasion of a third party's personal privacy.

34. The IPC found that STR hosts are required to operate STRs from their principle residence (i.e. their home) and must provide this address for their STR license.

Their home addresses would therefore be disclosed to the world if the Decision is not quashed.

35. An individual's home address is personal information that should not be subject to compelled public disclosure. An individual's license number can be associated with other personal information (such as full names, contact information, family member information or demographic information) available from other sources (including public Airbnb listings, other City records, databases, social media and search engines) to facilitate tracking and harassment of the STR operator. This concern is buttressed by the extensive evidence filed with the IPC by Airbnb reflecting the extent to which Airbnb hosts and their STR operators have been harassed by those who object to STRs like the Requestor.

36. The IPC held that because STR operators' home addresses could also be construed as business information that they do not constitute personal information subject to Section 22 of the *Act*.

37. The IPC erred in applying a binary distinction between personal information and business information. Even if the classification of STR operators' home addresses as business contact information was a reasonable finding, this does not render the information non-personal. The IPC erred in ignoring or discounting the relevant factors of the Section 22 analysis in considering the personal privacy impacts of disclosure of this information. This approach was unreasonable in light of the evidence establishing probable harm to STR operators if their personal information was disclosed.

38. The IPC erred in failing to consider the privacy impacts of the cumulative information between the Records that will be released if the Decision is not quashed, as well as the probable harm arising from the ability to associate this information with other publicly available information about STR operators.

39. In addition, the application of the Decision to future requests under the *Act* could cause even more significant harm to STR operators because of the IPC's error in determining that personal information when included in a record of a business license is no longer subject to Section 22 privacy protections. The effect of the Decision is that any personal information, such as names, phone numbers and email addresses, about individuals who hold STR licenses will be releasable to the world without consideration of whether it constitutes an invasion of privacy under the *Act*.

40. The IPC erred in failing to appropriately weigh the dual purposes of the *Act*: to provide access to information held by public bodies *and* to protect individuals' privacy. The consideration of the impact of disclosure on personal privacy must also take into account whether a request seeks information about individuals or about government decision-making, and the probability that personal information will be disseminated or published following disclosure.

The IPC Breached the Duty of Procedural Fairness and the Rules of Natural Justice

41. The IPC breached the duty of procedural fairness and the rules of natural justice by failing to provide notice of the Requests and the Decision to the STR operators whose privacy interests and rights under the *Act* are at issue.

42. The failure to provide notice of the proceeding or Decision to the very third parties whose privacy and safety is at issue constitutes a breach of the duty of procedural fairness and natural justice, and is a standalone basis on which to quash the decision.

43. Additionally, the breach compounds the errors described above and renders the Decision unreasonable on that basis as well. To the extent that the IPC was not prepared to rely on the evidence adduced by the City and Airbnb to demonstrate the applicability of Sections 15, 19 and 22 of the *Act*, it was incumbent on the City to provide the third parties whose privacy is at issue, who were best placed to demonstrate the impact of the proposed disclosure on them, and who will otherwise be directly impacted by the Decision, an opportunity to participate in the IPC proceeding.

44. The IPC's reliance on evidence of harm to the one individual who was a victim of stalking and had proactively reported her concerns, and holding that her information should not be disclosed, demonstrates that the IPC was required to give third party notice to all individuals whose information may be disclosed pursuant to the Decision. The STR operators had no positive duty to report such concerns to the City or Airbnb absent receiving notice of the potential disclosure in response to the specific requests of the Requester. It was unreasonable to deny them notice and rights of participation in a proceeding that impacted their personal information, privacy interests and security.

Additional Grounds

45. In addition, the Petitioner relies on the following legislative provisions and Supreme Court Civil Rules:

    (a) the provisions of the *Judicial Review Procedure Act*;[2] and

    (b) Rules 2-1(2)(b), 14-1, and 16-1 of the Supreme Court Civil Rules.

Part 4: MATERIAL TO BE RELIED ON

46. The Record of Proceedings before the IPC;

47. The Affidavit of Nathan Rotman sworn January 27, 2022; and

[2] , R.S.B.C. 1996, c. 241

48. Such further and other materials as counsel may advise and this Honourable court permit

The Petitioner estimates that the hearing of the Petition will take 1 day.

Date: January 27, 2022

Signature of ☐ Petitioner
☒ Lawyer for Petitioner

Molly Reynolds

To be completed by the court only:

Order made

☐ in the terms requested in paragraphs _____ of Part 1 of this petition

☐ with the following variations and additional terms:

_____

_____

_____

Date: _____ _____

Signature of ☐ Judge ☐ Master