IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia,* 2024 BCSC 2311

Date: 20241218
Docket: S220204
Registry: Vancouver

Between:

Clearview AI Inc.

Petitioner

And

Information and Privacy Commissioner for British Columbia

Respondent

Before: The Honourable Justice Shergill

On judicial review from: An order of the Information and Privacy Commissioner, dated December 14, 2021 (*Clearview AI Inc.*, [2021] B.C.I.P.C.D. No. 73).

Reasons for Judgment

Counsel for Petitioner:	E. Cribb D. Mitchell
Counsel for Respondent:	C. Parker, K.C. D. Wu
Counsel for Attorney General of British Columbia:	C. Rajotte C. Bant K. Reilly
Place and Dates of Hearing:	Vancouver, B.C. July 15-16, 2024
Place and Date of Judgment:	Vancouver, B.C. December 18, 2024

Table of Contents

I. OVERVIEW

[1] This case relates to the British Columbia Information and Privacy Commissioner's effort to regulate conduct of a United States based company that provides facial recognition services using images of individuals "scraped" from the Internet. The impugned images include those of people in British Columbia. The company provides its facial recognition services to third party customers, including law enforcement agencies.

[2] The Petitioner, Clearview AI Inc. ("Clearview"), voluntarily suspended its services to users in Canada in 2020, following the commencement of a joint investigation into its activities in Canada. However, the suspension is temporary, and Clearview has not committed to remaining out of the Canadian market beyond the end of the suspension period. Further, Clearview has continued to collect images and associated data of Canadians, including persons in British Columbia.

[3] In this Petition, Clearview seeks judicial review of a decision of the Information and Privacy Commissioner for British Columbia (the "Commissioner") titled Order P21-08 (the "*Decision*"[1]) which is dated December 14, 2021. The *Decision*:

1) prohibits Clearview from offering its facial recognition services to clients in British Columbia using images and biometric facial arrays ("personal information") collected from individuals in British Columbia without their consent;

2) orders Clearview to make best efforts to cease the collection, use, and disclosure of personal information collected from individuals in British Columbia without their consent; and

3) orders Clearview to make best efforts to delete personal information collected from individuals in British Columbia without their consent.

[1] Although the Decision is titled "Order", to avoid confusion, I will refer to the entire document as the "*Decision*" and the terms pronounced at para. 22 of the *Decision*, as the "Order".

(the "Order")

[4] Clearview seeks a declaration from this Court that the *Decision* is unreasonable; and an order quashing it and setting it aside. In support, Clearview argues that the Commissioner erred by:

a) concluding that the *Personal Information and Privacy Act* ("*PIPA"* or *"Act")*[2] applies to Clearview;

b) determining that the personal information collected by Clearview from publicly available websites published electronically, was not information that was "available to the public" pursuant to *PIPA* and related regulations ("*PIPA Regulations*")[3], and in any event, failing to provide adequate reasons justifying this conclusion;

c) finding that Clearview's purpose for collecting, using, and disclosing the personal information was not a purpose that "a reasonable person" would consider appropriate in the circumstances, and further failing to consider whether this interpretation of "reasonable purpose" within the meaning of *PIPA*, was consistent with the values set out in the Canadian *Charter of Rights and Freedoms* ("*Charter*")[4]; and

d) pronouncing an order that is unnecessary and unenforceable.

[5] The Commissioner defends the *Decision* and submits that it was reasonable. Consequently, there is no basis to quash the *Decision* or set it aside.

[6] The Attorney General of British Columbia's ("AGBC") participation in the proceeding was limited to two issues: (a) whether the Commissioner has jurisdiction over Clearview; and (b) whether the Commissioner was required to consider *Charter*

[2] *Personal Information and Privacy Act*, S.B.C. 2003, c. 63.
[3] *Personal Information Protection Act Regulations*, BC Reg 473/2003.
[4] The *Constitution Act, 1982,* Schedule B to the *Canada Act 1982 (UK),* 1982, c 11.

values when interpreting or applying ss. 11, 14, and 17 of *PIPA*. The AGBC agrees with the first proposition and disagrees with the second one.

[7] For the reasons that follow, this Petition is dismissed.

II. ISSUES

[8] The following issues are raised by the parties:

1. Does *PIPA* apply to Clearview?

2. Did the Tribunal err in its interpretation of “publicly available” or “reasonable purpose”?

3. Is the Order unnecessary, unenforceable, or overbroad?

[9] For clarity, Clearview is no longer challenging the constitutionality of *PIPA* in this proceeding. Nor is it seeking the declaration at paragraph 2 of Part 1 of the Petition, that ss. 11, 13, and 17 of *PIPA* unjustifiably infringe upon the right to freedom of expression enshrined in s. 2(b) of the *Charter*.

[10] It is also important to note here that when framing the issues concerning the interpretation of “publicly available” and “reasonable purpose” under *PIPA*, the parties have adopted short form terminology that is not actually present in the legislation or regulations. Rather than “publicly available” information, the *Act* refers to “personal information [that] is available to the public” and the *PIPA Regulations* refer to “sources of information available to the public”: *PIPA,* ss. 12(e), 15(e), 18(e); *PIPA Regulations*, s. 6. Further, instead of “reasonable purpose,” *PIPA* refers to “purposes that a reasonable person would consider are appropriate in the circumstances”: *PIPA*, ss. 11, 14, 17.

[11] However, the terms “publicly available” and “reasonable purpose” are used in a joint investigation report that plays a central role in this proceeding, and which is referenced later in these Reasons. For the sake of clarity and consistency, I adopt this same terminology in these Reasons. When necessary for accuracy, I will refer to the statutory language verbatim.

[12] Underlying each of the above issues is the question of the applicable standard of review. Before I address that, I will consider some preliminary matters.

III. PRELIMINARY MATTERS

[13] There are two preliminary matters that were raised by the parties. The first relates to the standing of the Commissioner to make fulsome submissions at this hearing; the second relates to the scope of this judicial review.

A. Should the Tribunal be Granted Standing to Make Submissions on the Merits?

[14] The Commissioner sought leave to participate fully in this judicial review proceeding and to make submissions on the merits. This request was unopposed. After considering the submissions of counsel and applicable authorities, I granted the Commissioner's request. I provide the following reasons in support.

[15] A tribunal's role in a judicial review proceeding where its own decision is at issue has traditionally been narrowly construed. For reasons of finality and impartiality, the tribunal is ordinarily limited to "an explanatory role with reference to the record before the Board and to the making of representations relating to jurisdiction": *Ontario (Energy Board) v. Ontario Power Generation Inc.*, 2015 SCC 44, at para. 42 ("*Ontario Energy Board*"), citing *Northwestern Utilities Ltd. v. City of Edmonton*, [1979] 1 S.C.R. 684, 1978 CanLII 17, at 709.

[16] However, there are circumstances in which more involved participation of the tribunal may be necessary to enable the reviewing court to make a fully informed adjudication of the issues before it. In such a case, it may be appropriate for the judge to exercise their discretion to permit the tribunal, which has specialized expertise and familiarity with the relevant administrative scheme, to make more fulsome submissions. These could include submissions about "how one interpretation of a statutory provision might impact other provisions within a regulatory scheme, or the factual and legal realities of the specialized field in which they work": *Ontario Energy Board*, at para. 53.

[17] Sometimes there may be no other party to stand in opposition to the party challenging the decision. In such a case, the participation of a tribunal as an adversarial party "may help the court ensure that it has heard the best of both sides of a dispute": *Ontario Energy Board*, at para. 54; see also *C.S. v. British Columbia (Workers' Compensation Appeal Tribunal),* 2019 BCCA 406, at paras. 47-48.

[18] Ultimately, tribunal standing is a matter to be determined by the court that is conducting the first-instance review. The court should exercise its discretion by balancing the need for fully informed adjudication against the importance of maintaining tribunal impartiality: *Ontario Energy Board*, at para. 57.

[19] In *Ontario Energy Board*, the Court set out the following factors at para. 59, which are relevant in informing the court's exercise of its discretion:

> (1) If an appeal or review were to be otherwise unopposed, a reviewing court may benefit by exercising its discretion to grant tribunal standing.
>
> (2) If there are other parties available to oppose an appeal or review, and those parties have the necessary knowledge and expertise to fully make and respond to arguments on appeal or review, tribunal standing may be less important in ensuring just outcomes.
>
> (3) Whether the tribunal adjudicates individual conflicts between two adversarial parties, or whether it instead serves a policy-making, regulatory or investigative role, or acts on behalf of the public interest, bears on the degree to which impartiality concerns are raised. Such concerns may weigh more heavily where the tribunal served an adjudicatory function in the proceeding that is the subject of the appeal, while a proceeding in which the tribunal adopts a more regulatory role may not raise such concerns.

[20] The following factors are present in the case at bar:

a) There is no other party to defend the reasonableness of the *Decision* as a whole.

b) The AGBC is participating only on discrete issues, and does not have the necessary knowledge and expertise to fully make and respond to the arguments raised on review.

c) Concerns about impartiality of the tribunal do not arise in relation to the issues before this Court, as the Commissioner did not act in an

> adjudicative capacity as an impartial arbiter of a dispute between two parties. Rather, this judicial review relates to the enforcement of an order that resulted from a joint investigation conducted by the Commissioner and others.

[21] Consequently, any concerns about tribunal impartiality are minimal, and outweighed by the need for fully informed adjudication.

[22] For these reasons, I have exercised my discretion to permit the Commissioner to participate fully in this judicial review, and provide submissions on the merits. Granting this request will assist this Court in arriving at a just outcome.

B. Should this Judicial Review Consider the Findings in the Joint Investigation Report?

[23] In its Petition Response, the Commissioner seeks to restrict the scope of this judicial review, through the following passages at Part 5: Legal Basis:

> 10. The main thrust of Clearview's argument that the interpretation of "publicly available" was unreasonable appears to be that the Offices did not provide adequate reasons for their interpretation (Petition, para. 11).
>
> 11. This is an attack on the findings of the Offices in the Joint Report, which Clearview has not judicially reviewed. These findings are not properly the subject of this judicial review proceeding.

[24] The Commissioner did not advance this argument at the hearing. However, they also did not expressly abandon it. For the sake of completion, I have addressed it below.

[25] The joint investigation report (the “Report”) referenced in the Petition Response was prepared by the federal privacy commissioner, and the privacy commissioners of British Columbia, Quebec, and Alberta (collectively the “Privacy Commissioners”), following the completion of a joint investigation into the activities of Clearview in Canada (the “Investigation”). [5] The Report summarizes the findings in

[5] *Decision*, Appendix A, Joint Investigation Report by the Privacy Commissioner of Canada (OPC), the Commission d’accès à l’information du Québec (CAI), the Information and Privacy Commissioner for British Columbia (OIPC BC), and the Information and Privacy Commissioner of Alberta (OIPC AB)

the Investigation and made various recommendations. No binding or reviewable decision was made in the Report. Thus, the Report does not offer a standalone basis for judicial review.

[26] Further, the Commissioner expressly adopted the reasoning in the Report by including it as part of the Decision.[6] Indeed, the Commissioner relied heavily on the reasoning in the Report during this hearing.

[27] As held in *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65 ("*Vavilov*"), at para. 119, formal reasons for a decision may take different forms. In this case, while the Report is not contained in the body of the *Decision* itself, it is attached as Appendix A to the *Decision* and expressly incorporated into it.

[28] I am satisfied that the Report forms part of the *Decision*. It is therefore properly before this Court for consideration on this judicial review.

IV. STANDARD OF REVIEW

[29] The parties agree that under the framework established by the Supreme Court of Canada in *Vavilov*, the presumptive standard of review of the Commissioner's decision is reasonableness. This presumptive standard can be rebutted when the legislature intends a different standard to apply, or the rule of law requires that the standard of correctness be applied: *Sharp v. Autorité des marchés financiers*, 2023 SCC 29, at para. 37, citing *Vavilov*, at paras. 16-17.

[30] The correctness standard applies to: (a) cases involving constitutional questions; (b) general questions of law which are of central importance to the legal system as a whole; and (c) questions related to jurisdictional boundaries between two or more administrative bodies: *Sharp*, at para. 37; *Vavilov*, at para. 17.

---

into Clearview AI Inc.'s compliance with *the Personal Information Protection and Electronic Documents Act (*PIPEDA), the *Act Respecting the Protection of Personal Information in the Private Sector*, the *Act to Establish a Legal Framework for information Technology* (LCCJTI), the *Personal Information Protection Act* (PIPA BC), and the *Personal Information Protection Act* (PIPA AB).

[6] *Decision*, para. 2.

[31] When a party raises issues about the jurisdiction of an administrative tribunal over an out-of-province party, this raises a constitutional issue regarding the territorial reach of provincial legislation. Hence, the correctness standard applies: *Sharp*, at para. 38.

[32] Matters of statutory interpretation, on the other hand, should not be treated differently than other questions of law. These are reviewed on a standard of reasonableness: *Vavilov*, at para. 115.

[33] The parties agree that: (a) the question of whether *PIPA* applies to Clearview raises a jurisdictional question, and thus the correctness standard applies; and (b) issues about the Commissioner's interpretation of *PIPA* are to be reviewed applying the reasonableness standard.

[34] The parties disagree on the applicable standard of review related to the *Charter* values argument. The Petitioner argues that like other Constitutional questions, questions of *Charter* values should be determined on a correctness standard; the Commissioner submits that even though *Charter* values are raised, this is fundamentally a matter of statutory interpretation to which the reasonableness standard applies.

[35] In *Doré v. Barreau du Québec,* 2012 SCC 12, the Court held that "the fact that *Charter* interests are implicated does not argue for a different standard" than that of reasonableness: at para. 45. This view was reiterated in *Vavilov*, where the Court emphasized the distinction between cases in which it is alleged that an administrative decision infringed on *Charter* rights and cases in which it is alleged that the enabling statute violates rights. The former are held to a reasonableness standard while the latter attract correctness: *Vavilov*, at para. 57.

[36] I agree with the Commissioner that, like other matters of statutory interpretation, Clearview's *Charter* values arguments should be reviewed on a reasonableness standard: *Vavilov*, at para. 115.

[37] I turn now to the background facts that are relevant to this proceeding.

V. FACTUAL BACKGROUND

[38] The following facts are uncontroverted.

A. Clearview

[39] Clearview is a company based in the United States that provides government and law enforcement agencies with facial recognition search engine services. It does this through a facial recognition software which utilizes an automated tool called an "image crawler". The image crawler scans the internet for images of human faces that people have posted online.

[40] Clearview's facial recognition tool functions in four key sequential steps.[7]

[41] First, Clearview "scrapes" images of faces and associated metadata (such as title, source link and description) from online sources, including social media. These images and metadata are downloaded and stored indefinitely on Clearview's servers.

[42] Second, Clearview uses an algorithm (underpinned by the "neural network") to analyze digital images of faces and create biometric identifiers in the form of numerical representations for each image. These numerical representations are called "vectors". Clearview's vectors consist of 512 data points that represent the various unique lines that make up a face. These vectors are stored in a database where they are associated with the images stored on Clearview's server. Every image in the database has a vector associated with it in order to allow identification and matching.

[43] Third, Clearview provides its clients with an App which allows users to search the Clearview database to identify a specific "target". An App user who wishes to identify an individual must upload an image of their target into the App. This image is analyzed by the neural network which produces a vector. This vector is compared

[7] Report, pp. 7-8, paras. 13-15.

against all vectors stored in Clearview's database. The App pulls any matching images from the vector.

[44] Finally, Clearview provides a list of search results to the client. This list contains thumbnail images that appear to be a match for an individual, as well as the metadata associated with the images (i.e. name of the image, a description, and source link). If a user wishes to obtain additional information about the person, they can do so by clicking on to the associated source link. They are then re-directed to the source page where the image was originally collected.

[45] Through this process, Clearview has amassed a database of more than three billion images of faces and corresponding biometric identifiers. As found by the Privacy Commissioners, this "practice of indiscriminate scraping has undoubtedly resulted in the collection of the personal information of individuals within … British Columbia", including children.[8] Clearview does not deny that its database includes personal information belonging to people in British Columbia.

B. Investigation

[46] In January and February 2020, there were multiple public reports indicating that Clearview was populating its facial recognition database by collecting digital images of people's faces from a variety of public websites, including Facebook, YouTube, Instagram, Twitter, and Venmo. These images were being collected without the consent of the individuals, and in apparent violation of the terms of service of those websites. There were also various media reports that Canadian law enforcement agencies and private organizations were using Clearview's services to identify individuals.[9]

[47] In February 2020, the Commissioner, along with the Office of the Privacy Commissioner of Canada ("OPC"), the Commission d'accès à l'information du Québec ("CAI"), and the Information and Privacy Commissioner of Alberta ("OPC

[8] Report, pp. 2 and 12.
[9] Report, p. 6, paras. 3-4.

AB"), decided to commence a joint investigation into Clearview's services in Canada (the "Investigation").[10]

[48] The Investigation was initiated pursuant to the statutory authority governing each privacy commissioner (the "*Acts*"). In British Columbia, the relevant authority is contained at s. 36(1)(a) of *PIPA*.

[49] The purpose of the Investigation was to examine whether Clearview's collection, use, and disclosure of personal information by means of its facial recognition tool complied with federal and provincial privacy laws applicable to the private sector.[11]

[50] The Privacy Commissioners identified the following issues to be investigated:

a) Whether Clearview was required under the *Acts* to get consent for its collection, use and disclosure of personal information and if so, whether it did; and

b) Whether Clearview collected, used and/or disclosed personal information for an appropriate purpose within the meaning of the *Acts*.

[51] During the course of the Investigation, the Privacy Commissioners conducted extensive open-source research, and sought submissions and records from Clearview and other third parties. Clearview was also provided opportunities to meet with the Privacy Commissioners, make inquiries, and provide additional evidence.

[52] In July 2020, Clearview decided to voluntarily exit from the Canadian market. However, Clearview indicated that it intended to return to the Canadian market at some point in the future.

[10] Ibid., para. 5.
[11] Ibid. p. 3.

C. Report

[53] The Privacy Commissioners published their Report on the Investigation on February 3, 2021.

[54] In the Report, the Privacy Commissioners concluded that Clearview did not obtain the requisite consent to collect, use and disclose the personal information of Canadians. In relation to British Columbia, the Privacy Commissioners found these activities violated ss. 6 - 8 of *PIPA*.[12] They also concluded that Clearview had collected, used and disclosed personal information for an improper purpose, thereby contravening ss. 11, 14, and 17 of *PIPA*.[13]

[55] The Privacy Commissioners made the following three recommendations to Clearview:

1) cease offering the facial recognition services that were the subject of the investigation, to clients in Canada;

2) cease the collection, use and disclosure of personal information collected from individuals in Canada; and

3) delete personal information collected from individuals in Canada in its possession.

(the "Recommendations") [14]

[56] At the conclusion of the Report, the Privacy Commissioners advised Clearview that if it continued to refuse to accept their findings and Recommendations, they would pursue other actions available under their respective *Privacy Acts*[15] to bring Clearview into compliance with federal and provincial privacy laws applicable to the private sector.[16]

---

[12] Report, para. 118.
[13] *Decision*, paras. 6-7; Report, at para. 119.
[14] *Decision*, para. 8.
[15]These privacy acts are: the *Personal Information Protection and Electronic Documents Act (*PIPEDA), the *Act Respecting the Protection of Personal Information in the Private Sector*, the *Act to Establish a Legal Framework for information Technology* (LCCJTI), the *Personal Information Protection Act* (PIPA BC), and the *Personal Information Protection Act* (PIPA AB).
[16] Report, para. 123.

[57] Between April 2021 and October 2021, the Privacy Commissioners engaged with Clearview to ascertain its willingness and/or ability to comply with the Recommendations.

[58] With respect to Recommendation 1, Clearview stated that it had ceased providing services to Canadian clients since 2020 and was willing to continue this undertaking for a further 18 months. In the event it did return to Canada, Clearview offered to provide an audit trail of the searches conducted, and to require a facial recognition policy of each of its clients.

[59] Regarding Recommendations 2 and 3, Clearview took the position that these were "impossible to execute", and in any event, were not legally warranted. According to Clearview, it was not possible, merely from photographs, to identify whether the individuals in the photographs were in Canada at the time the impugned photograph was taken, or whether they were Canadian citizens, residents of Canada, etc. Further, Clearview argued that use of the photographs was permissible under Canadian law as the photographs were "publicly available". [17]

[60] In September 2021, the Commissioner wrote to Clearview to address concerns that were specific to British Columbia. The Commissioner asked Clearview why it could not implement measures to delete or limit the collection of information from British Columbia, similar to the measures it submitted it could take in court proceedings in Illinois.

[61] Clearview responded in October 2021, explaining that the measures it proposed in Illinois are "very rough proxies" to assist in determining that the individuals in a photograph may be in or from the state, as they primarily identified where a photograph was taken rather than the residence of the individuals in the photograph. As such, Clearview argued that even if the Illinois measures were replicated with respect to British Columbia, this would not ensure compliance with the terms of the recommendations of the Privacy Commissioners.

[17] The reference to Canada in this paragraph includes British Columbia.

VI. THE DECISION

[62] The Commissioner considered Clearview's arguments about why it could not (or need not) comply with the Recommendations. He concluded that Clearview did not have valid reasons for non-compliance, and issued a binding order on December 14, 2021. The *Decision* is indexed at *Clearview AI Inc.,* 2021 BCIPC 73.

[63] The Commissioner's authority to make the Order comes from s. 36 of *PIPA*. Section 36(1)(b) empowers the Commissioner to make an order described in s. 52(3). Under s. 52(3)(e) the Commissioner may require an organization to "stop collecting, using or disclosing personal information" in contravention of the *Act*. Section 52(3)(f) permits the Commissioner to require an organization to destroy personal information which is collected in contravention of the *Act*.

[64] The terms of the Order are set out at paragraph 22 of the *Decision*, as follows:

> [22] Pursuant to s. 36(1)(b) of BC *PIPA*, the [sic] I make the following order:
>
> a. Clearview is prohibited from offering its facial recognition services that have been the subject of the investigation, and which utilize the collection, use and disclosure of images and biometric facial arrays collected from individuals in British Columbia without their consent, to clients in British Columbia;
>
> b. Clearview shall make best efforts to cease the collection, use and disclosure of (i) images and (ii) biometric facial arrays collected from individuals in British Columbia without their consent; and
>
> c. Clearview shall make best efforts to delete the (i) images and (ii) biometric facial arrays in its possession, which were collected from individuals in British Columbia without their consent.
>
> [23] Section 53(1) of BC *PIPA* requires the Organization to comply with the orders in the previous paragraph by no later than January 25, 2022. As a condition under s. 52(4) of PIPA, I require the Organization to provide the OIPC Registrar with written evidence of its compliance with the above orders by January 25, 2022.

[65] The *Decision* details the Commissioner's reasons for making the Order. I will deal with those in my Reasons, as they arise.

[66] I turn now to the first issue raised in this judicial review, that of jurisdiction.

VII. DOES *PIPA* APPLY TO CLEARVIEW?

[67] As stated earlier, the issue of *PIPA's* application to Clearview is a jurisdictional question to which the correctness standard of review applies.

[68] The correctness standard was explained by the majority of the Court in *Vavilov* as follows:

> [54] When applying the correctness standard, the reviewing court may choose either to uphold the administrative decision maker's determination or to substitute its own view: *Dunsmuir*, at para. 50. While it should take the administrative decision maker's reasoning into account — and indeed, it may find that reasoning persuasive and adopt it — the reviewing court is ultimately empowered to come to its own conclusions on the question.

[69] For the reasons that follow, I conclude that the Commissioner correctly found that *PIPA* applies to Clearview's activities.

[70] The parties agree that the test articulated by the Supreme Court of Canada in *Unifund Assurance Co. v. Insurance Corp. of British Columbia*, 2003 SCC 40 ("*Unifund*") is the appropriate test to determine whether provincial regulatory legislation is constitutionally applicable to out of province parties.

[71] In *Unifund*, Justice Binnie examined the approach to be taken when considering the validity of extraterritorial application of a provincial statute within Canada. He confirmed that "[t]he territorial limits on the scope of provincial legislative authority prevent the application of the law of a province to matters not sufficiently connected to it": *Unifund*, at para. 58.

[72] Justice Binnie formulated the following test for when provincial legislation applies to an out of province individual or entity:

> 56 Consideration of constitutional *applicability* can conveniently be organized around the following propositions:
>
> 1. The territorial limits on the scope of provincial legislative authority prevent the application of the law of a province to matters not sufficiently connected to it;
> 2. What constitutes a "sufficient" connection depends on the relationship among the enacting jurisdiction, the subject matter of the legislation and the individual or entity sought to be regulated by it;

3. The applicability of an otherwise competent provincial legislation to out-of-province defendants is conditioned by the requirements of order and fairness that underlie our federal arrangements;
4. The principles of order and fairness, being purposive, are applied flexibly according to the subject matter of the legislation.

[73] The *Unifund* test was applied by the British Columbia Court of Appeal to determine whether the securities commission had jurisdiction over out of province defendants who allegedly breached the securities legislation: *McCabe v. British Columbia (Securities Commission),* 2016 BCCA 7, at paras. 34-37.

[74] More recently in *Sharp*, the Court affirmed that the territorial reach of provincial legislation is to be interpreted in accordance with the *Unifund* decision: *Sharp,* at paras. 104-105.

[75] Consequently the “real and substantial connection” test in *Unifund* is now the “accepted test for discerning the presumptively intended reach of federal legislation as well as the constitutionally permissible application of provincial legislation”: *Sharp*, at para. 110, citing Ruth Sullivan, *The Construction of Statutes*, 7th ed. (Markham: LexisNexis Canada, 2002), at 806.

A. Did the Tribunal Correctly Find a Real and Substantial Connection Exists?

[76] In the *Decision*, the Commissioner noted that Clearview has obtained personal information belonging to Canadians and offered its services to clients in Canada: *Decision*, at paras. 4-5. Furthermore, the *Decision* relies upon and expressly adopts the Report, which explicitly found a “real and substantial connection” to Canada exists and rejected any argument that Clearview is not subject to provincial privacy legislation: Report, at paras. 28, 32-35. Clearview relies on *Sharp* to support its position that the Commissioner was wrong in this conclusion.

[77] According to Clearview, the “fundamental basis” on which sufficient connection was established in *Sharp*, was the fact that the out of province parties had been engaged in business activities in Québec, which is not the case here.

[78] I disagree with this interpretation of *Sharp*. In my view, neither *Sharp*, nor indeed *Unifund*, are to be read so narrowly. Both cases emphasize the need for a contextual analysis. To that end, as noted by the majority in *Sharp*:

> [127] The first two principles in *Unifund* are related. The first principle requires a sufficient connection, while the second principle identifies factors that might furnish that connection (Sullivan, at p. 822). This involves a contextual inquiry. As Binnie J. noted in *Unifund*, "different degrees of connection to the enacting province may be required according to the subject matter of the dispute" (para. 65). In each case, a court or tribunal must examine the relationship among the enacting jurisdiction, the subject matter of the law, and the person sought to be regulated by it, to decide whether that relationship is sufficient to support the applicability of the legislation to the out-of-province person (para. 65).

[79] The subject matter at issue in this case is different than what concerned the Court in *Unifund* and *Sharp*. The case at bar deals with the protection of privacy. The *Unifund* and *Sharp* cases concerned themselves with insurance and securities regulations, respectively. Thus, in *Sharp*, the fact that securities were partly marketed in Québec through a company which was a reporting issuer in Québec, was of central importance to establish sufficient connection: *Sharp,* at para. 129. In contrast, the absence of the Insurance Corporation of British Columbia marketing insurance in Ontario militated against a finding of real and substantial connection in the *Unifund* case: *Unifund*, at para. 84.

[80] Privacy legislation raises uniquely different considerations than insurance and securities regulations. Nevertheless, to the extent that *Sharp* stands for the proposition that out of province parties must be engaged in business activities in the province to meet the *Unifund* test, that requirement is met in this case.

[81] The record before the Commissioner supports the finding that Clearview has in fact provided its services to entities in British Columbia and carried out business and marketing in the province. In a letter dated June 3, 2020, Clearview attached various documents, including a list of Canadian user organizations. The user organizations included municipal police departments located in the following cities in British Columbia: Vancouver, Victoria, New Westminster, and Port Moody. In addition, the Royal Canadian Mounted Police ("RCMP"), which was a paying client

of Clearview's, has jurisdiction over many regions in British Columbia. It also appears from that same letter that Clearview distributed its marketing materials to entities in British Columbia through the "CrimeDex Alert System".

[82] Thus, Clearview's characterization of the "fundamental basis" on which sufficient connection was found to exist in *Sharp* is also present in this case. Clearview collected, used, and disclosed information of individuals in British Columbia and provided its services to a number of entities in the province.

[83] The Commissioner was also correct to conclude that Clearview's voluntary suspension of Canadian accounts and promise not to enter the Canadian market for a specified period of time, did not impact the Commissioner's jurisdiction. As the Commissioner put it so aptly:

> The constitutional application of provincial regulatory schemes cannot turn on voluntary decisions made by organizations in the midst of an investigation pursuant to that same regulatory scheme. It would mean that an organization could remove itself from the ambit of regulatory authority in the middle of an investigation at its own initiative, re-enter the market after the regulator "loses jurisdiction", and then do the same if an investigation is commenced again.[18]

[84] In addition, even if Clearview no longer offers its services to British Columbia companies or residents, this does not mean that it has ceased conducting business in the province.

[85] In *Equustek Solutions Inc. v. Jack*, 2014 BCSC 1063 ("*Equustek*"), Justice Fenlon, then of this Court, found that British Columbia courts had territorial competence over Google because it carried on "business" in British Columbia. In coming to that conclusion, she gave weight to the fact that:

> [49] Google collects a wide range of information as a user searches, including the user's IP address, location, search terms, and whether the user acts on the search results offered by "clicking through" to the websites on the list.
>
> [50] In addition to its search services, Google sells advertising to British Columbia clients.

[18] Commissioner Brief of Argument, para. 82.

[86] The Court of Appeal endorsed that analysis in *Equustek Solutions Inc. v. Google Inc.,* 2015 BCCA 265, and expanded it further as follows:

> [54] While Google does not have servers or offices in the Province and does not have resident staff here, I agree with the chambers judge's conclusion that key parts of Google's business are carried on here. The judge concentrated on the advertising aspects of Google's business in making her findings. In my view, it can also be said that the gathering of information through proprietary web crawler software ("Googlebot") takes place in British Columbia. This active process of obtaining data that resides in the Province or is the property of individuals in British Columbia is a key part of Google's business.
>
> [55] Google says that even if it is concluded that it carries on business in British Columbia, the injunction was not properly granted, because it did not relate to the specific business activities that Google carries on in the Province. In my view, the business carried on in British Columbia is an integral part of Google's overall operations. Its success as a search engine depends on collecting data from websites throughout the world (including British Columbia) and providing search results (accompanied by targeted advertising) throughout the world (including British Columbia). The business conducted in British Columbia, in short, is the same business as is targeted by the injunction.
>
> [Emphasis added]

[87] I accept that the *Equustek* case is distinguishable insofar as it dealt with "adjudicatory jurisdiction" rather than "prescriptive legislative jurisdiction". Those two concepts were held by the court in *Sharp* to be distinct from each other: *Sharp*, at paras. 115-116. However, the Court's analysis in *Equustek* of how to view "business" when examining organizations which use data from the Internet, is instructive and consistent with the Federal Court's approach in *A.T. v. Globe24h.com*, 2017 FC 114. The *A.T.* decision is cited in the Report and relied on by Clearview.

[88] In *A.T.*, the Federal Court found that federal privacy legislation ("*PIPEDA*")[19] applied to a website based in Romania. The Court noted that the content at issue contained personal information sourced from Canadian legal websites, that the website targeted a Canadian audience, and that it impacted the Canadian public: *A.T.,* at para. 55. While the website operator and host server were located abroad,

[19] *Personal Information Protection and Electronic Documents Act*, S.C. 200, c. 5.

the Court also held that "the physical location of the website operator or host server is not determinative": *A.T.,* at para. 54.

[89] More recently in *Facebook, Inc. v. Canada (Privacy Commissioner),* 2023 FC 534 ("*Facebook*"), the Federal Court found that the *Unifund* test was satisfied in relation to *PIPEDA* in circumstances where an American company was accessing the data of Canadian users. The Ontario Privacy Commissioner investigated data sent by Facebook to Cambridge Analytica. In finding that the real and substantial connection test had been met, the Court reasoned that there are millions of Facebook users in Canada, and data sent to Cambridge Analytica included data from these Canadian Facebook users: *Facebook*, at para. 86.

[90] The above authorities support the proposition that the *Unifund* test can be met merely by collecting data from individuals in British Columbia through the Internet.

[91] I agree with the Commissioner that it is too narrow of an analysis to simply look at whether Clearview has any employees, offices, or servers in British Columbia. As with Google, an essential part of Clearview's business is to collect data from websites like Facebook, YouTube, and Instagram. The ubiquitous presence of these websites leads to the logical inference that they undoubtedly have hundreds of thousands, if not millions, of users in British Columbia.

[92] Even if it were incorrect to conclude that Clearview does business in British Columbia by marketing and providing its services to entities in the province, there is still sufficient basis to find a real and substantial connection. The fact remains that Clearview collects, uses, and discloses personal information of individuals in British Columbia, which it gathers from the internet.

[93] The Commissioner was alive to this, noting in the *Decision* that Clearview "amassed a database of over three billion images of faces and corresponding biometric identifiers, including those of a vast number of individuals in Canada, including children": *Decision*, at para. 4. The Report also found that Clearview's business model "undoubtedly" resulted in the collection of personal information

belonging to individuals in British Columbia: Report, at para. 33. In light of this, the Report found the company could not "evade" obligations under provincial statutes: Report, at para. 34.

[94] In *Sharp* the court noted the "transnational nature of modern securities regulation and the public interest in addressing international market manipulation" as being significant to the "sufficient connection" analysis: *Sharp*, at para. 128. While this comment was made in the context of securities regulation, this sentiment has equal application to the privacy legislation sphere.

[95] In *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401,* 2013 SCC 62 ("*United Foods*") the Court explained the important role that privacy plays in the preservation of our societal values, the "quasi-constitutional" status afforded to privacy legislation, and the increasing significance of privacy laws as technology advances:

> [19] The focus is on providing an individual with some measure of control over his or her personal information... The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society: ...
>
> [20] *PIPA*'s objective is increasingly significant in the modern context, where new technologies give organizations an almost unlimited capacity to collect personal information, analyze it, use it and communicate it to others for their own purposes.

[96] Although *United Foods* was concerned with Alberta's privacy legislation, that legislation has similar objectives to British Columbia's *PIPA*.

[97] *PIPA* protects the ability of people in British Columbia to control their personal information by imposing restrictions on the collection, use and disclosure of information related to them. This becomes even more pressing with the ubiquitous presence of the internet and the profoundly intrusive impact it has on our daily lives.

[98] Informational privacy was also at issue in *R. v. Bykovets,* 2024 SCC 6, albeit in the context of the right to be free from unreasonable search and seizure under s. 8 of the *Charter*. In *Bykovets*, the majority of the Court held that there is a reasonable expectation of privacy over one's IP address. In arriving at its decision, the Court explained the nature of informational privacy, as follows:

> [32] This case is about informational privacy, or "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (*Tessling*, at para. 23, quoting A. F. Westin, Privacy and Freedom (1970), at p. 7). In other words, this aspect of privacy is concerned with "informational self-determination" (*Jones*, at para. 39).

[99] As noted by the court in *Bykovets* at para. 5, the "architecture of the Internet has led to a broad, accurate, and continuously expanding permanent record 'without precedent in our society'". Private corporations have "immense informational power" because the Internet has allowed them to track their users and "build profiles of their users filled with information the users never knew they were revealing": *Bykovets*, at para. 75-76. These concerns are heightened when private third parties work with law enforcement:

> [78] By concentrating this mass of information with private third parties and granting them the tools to aggregate and dissect that data, the Internet has essentially altered the topography of privacy under the *Charter*. It has added a third party to the constitutional ecosystem, making the horizontal relationship between the individual and the state tripartite. Though third parties are not themselves subject to s. 8, they "mediat[e] a relationship which is directly governed by the *Charter* — that between the defendant and police" (A. Slane, "Privacy and Civic Duty in R v Ward: The Right to Online Anonymity and the Charter-Compliant Scope of Voluntary Cooperation with Police Requests" (2013), 39 *Queen's L.J.* 301, at p. 311).
>
> [79] That shift has enhanced, rather than constrained, the state's informational capacity. "[T]echnological developments are permitting government actors to expand their surveillance powers significantly, in part by tapping into detailed information collected by the private sector" (A. J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" (2003), 29 *Queen's L.J.* 364, at p. 406). Professor Austin describes this state of affairs as the "new public/private nexus of surveillance", where intermediaries can "allo[w] the state to access the content of our communications as well as a treasure trove

> of other associated data" (p. 453). As a result, "in the context of intermediary cooperation state power is augmented" (p. 458).[20]

[100] Our courts have long recognized the uniquely different concerns raised by online spaces versus physical spaces. As held in *Bykovets* at para. 49, digital subject matter does not fit easily within traditional notions of "territorial privacy". This has led the courts to apply different factors to establish real and substantial connection when it comes to the Internet.

[101] For example, in *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers,* 2004 SCC 45 ("*SOCAN"*), the Court held at para. 61:

> In terms of the Internet, relevant connecting factors would include the situs of the content provider, the host server, the intermediaries and the end user. The weight to be given to any particular factor will vary with the circumstances and the nature of the dispute.

[102] Applying the factors in *SOCAN*, the Court in *A.T.* noted that even though the website operator and host server in question were based in Romania, the physical location was not determinative: *A.T.,* at para. 54. Similarly, the fact that Clearview is physically based in the United States is not determinative of whether a sufficient connection exists.

[103] After considering the applicable authorities, the subject matter of *PIPA,* and Clearview's activities, I find that the Commissioner correctly concluded that a real and substantial connection exists between Clearview's activities and British Columbia.

B. Did the Tribunal Correctly Apply the "Order and Fairness" Factors?

[104] I turn then to the third and fourth aspects of the *Unifund* test. I find that these too are satisfied in this case, such that the Commissioner was correct in applying *PIPA* to Clearview. The "order and fairness" factors were discussed in *Sharp* as follows:

[20] *Bykovets*, paras. 78-79.

> [131] The third and fourth *Unifund* principles are also related and "incorporate the notions of interprovincial comity and fairness to the defendant" (*Sullivan*, at p. 822). The third principle requires a court or tribunal to consider the principles of order and fairness, which function "as a mechanism to regulate extraterritoriality concerns" (*Unifund*, at para. 73) by ensuring the "security of transactions with justice" (para. 68, citing *Morguard*, at p. 1097). "Order" refers to the idea that courts and tribunals must respect the principle of interprovincial comity and only assume jurisdiction where constitutionally appropriate (*Unifund*, at para. 71; *Morguard*, at p. 1102). "Fairness" refers to fairness to the out-of-province defendant (*Unifund*, at para. 72; *Morguard*, at p. 1103). Finally, the fourth *Unifund* principle requires a court or tribunal to apply the principles of order and fairness purposively and flexibly given the subject matter of the legislation and the type of jurisdiction being asserted (*Unifund*, at para. 80).

[105] The application of *PIPA* to Clearview does not offend the principle of order or international comity. Just as securities regulation needs to be increasingly cross-border in nature, so too does privacy regulation. As the Court held in *Sharp* in regard to securities regulation:

> [134] Given the cross-border nature of securities manipulation and securities fraud, regulators from multiple jurisdictions may exercise jurisdiction over the same scheme. As noted by the intervener the Ontario Securities Commission, this is "a feature, not a flaw" of modern securities regulation (I.F., at para. 15). "It promotes the seamless coverage of regulatory protection and the imposition of public interest remedies across the territories affected by a single, unlawful scheme" (para. 15). We also agree with the AMF: [TRANSLATION]". . . nothing precludes such a multiplicity of proceedings because each of the proceedings constitutes a legitimate exercise of the jurisdiction of the state concerned. . . . [T]he application of the sufficient connection test is not a zero-sum game" (R.F., at paras. 81 and 87).

[106] Similar considerations apply to privacy legislation.

[107] I find also that there is nothing unfair about having *PIPA* apply to Clearview. Clearview chose to enter British Columbia and market its product to local law enforcement agencies. It also chooses to scrape data from the Internet which involves personal information of people in British Columbia.

[108] In my view, there is a significant public interest in addressing the transnational privacy issues raised by the facial recognition software services provided by Clearview. Those services rely in part on personal information collected from people in British Columbia.

[109] In summary, the Commissioner was correct in finding that *PIPA* applies to Clearview and that he has the jurisdiction to pronounce orders to regulate Clearview's conduct as it relates to personal information of persons in British Columbia.

VIII. DID THE TRIBUNAL ERR IN ITS INTERPRETATION OF "PUBLICLY AVAILABLE" OR "REASONABLE PURPOSE"?

[110] Clearview raises two arguments on the merits of the *Decision*. The first relates to whether the Commissioner's interpretation of information that was "available to the public" (or "publicly available") is unreasonable. Second, whether Clearview had "purposes that a reasonable person would consider appropriate in the circumstances" (or a "reasonable purpose") for the use, collection, and disclosure of personal information.

[111] To provide context, it is helpful to set out the applicable statutory framework.

A. Statutory Framework

[112] *PIPA* is concerned with the collection, use, and disclosure of "personal information" of an individual by an organization.

[113] The purpose of *PIPA* is explained in s. 2:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[114] Part 3 of *PIPA* relates to consent. Section 6 prohibits an organization from collecting, using, or disclosing personal information about an individual without their consent, except in certain specified situations. The specific terms of the provision are as follows:

> **Consent required**
>
> **6**(1) An organization must not
>
> (a) collect personal information about an individual,

(b) use personal information about an individual, or

(c) disclose personal information about an individual.

(2) Subsection (1) does not apply if

(a) the individual gives consent to the collection, use or disclosure,

(b) this Act authorizes the collection, use or disclosure without the consent of the individual, or

(c) this Act deems the collection, use or disclosure to be consented to by the individual.

[115] Consent can be express or deemed. Express consent is valid only if it meets the requirements of ss. 7 and 10 of the *Act*: *Bellevue West Building Management Ltd. (Re),* 2022 BCIPC 74, at para. 9.

[116] The following provisions in ss. 7 and 10 are relevant to determining whether an organization has express consent pursuant to s. 6(2)(a):

Provision of consent

7(1) An individual has not given consent under this Act to an organization unless

(a) the organization has provided the individual with the information required under section 10 (1), and

(b) the individual's consent is provided in accordance with this Act.

…

…

10(1) On or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing

(a) the purposes for the collection of the information, and

(b) on request by the individual, the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.

…

(3) This section does not apply to a collection described in section 8 (1) or (2).

[117] Section 10 is found under Part 4 of *PIPA*, which places limits on an organization's ability to collect personal information. If there is no deemed consent, then s. 10 provides that an organization collecting personal information must disclose to the individual the purposes for its collection.

[118] To determine whether deemed consent has been obtained under s. 6(2)(c) one must consider s. 8. The relevant provisions are as follows:

> **Implicit consent**
>
> **8**(1) An individual is deemed to consent to the collection, use or disclosure of personal information by an organization for a purpose if
>
> (a) at the time the consent is deemed to be given, the purpose would be considered to be obvious to a reasonable person, and
>
> (b) the individual voluntarily provides the personal information to the organization for that purpose.
>
> …
>
> (3) An organization may collect, use or disclose personal information about an individual for specified purposes if
>
> (a) the organization provides the individual with a notice, in a form the individual can reasonably be considered to understand, that it intends to collect, use or disclose the individual's personal information for those purposes,
>
> (b) the organization gives the individual a reasonable opportunity to decline within a reasonable time to have his or her personal information collected, used or disclosed for those purposes,
>
> (c) the individual does not decline, within the time allowed under paragraph (b), the proposed collection, use or disclosure, and
>
> (d) the collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances.
>
> (4) Subsection (1) does not authorize an organization to collect, use or disclose personal information for a different purpose than the purpose to which that subsection applies.
>
> …

[119] To determine whether s. 6(2)(b) applies, such that no consent is required, one must also consider ss. 11 and 12(1) of the *Act*.

[120] Section 11 limits the collection of personal information as follows:

> **Limitations on collection of personal information**
>
> 11 Subject to this Act, an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> (a) fulfill the purposes that the organization discloses under section 10 (1), or
>
> (b) are otherwise permitted under this Act.

[121] Section 12 provides a list of circumstances where an organization can collect personal information without consent or from a source other than the individual. The relevant provision in this case is s. 12(1)(e), which provides:

> 12(1) An organization may collect personal information about an individual without consent or from a source other than the individual, if
>
> …
>
> (e) the personal information is available to the public from a source prescribed for the purposes of this paragraph,

[122] Part 5 of *PIPA* places similar limits on the use of personal information, to those limits contained at ss. 11 and 12 governing the collection of personal information.

[123] The wording of s. 14 is virtually identical to s. 11, except that the limitations relate to the use of personal information. Section 14 also contains a clause to address the use of personal information that was collected before *PIPA* came into force, as follows:

> **Limitations on use of personal information**
>
> **14** Subject to this Act, an organization may use personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> (a) fulfill the purposes that the organization discloses under section 10 (1),
>
> (b) for information collected before this Act comes into force, fulfill the purposes for which it was collected, or
>
> (c) are otherwise permitted under this Act.

[124] Like s. 12(1), s. 15(1) further limits when an organization may disclose personal information without the individual's consent. The language of s. 15(1)(e) is virtually identical to s. 12(1)(e), except that it relates to what an organization "may use" rather than "may collect".

[125] Part 6 of *PIPA* governs the disclosure of personal information. As with Part 5, the language of the relevant provisions is virtually identical to ss. 11 and 12.

[126] Section 17 restricts disclosure of personal information to circumstances in which there is a reasonable purpose. It mirrors the language of s. 14, except that "may use" is replaced with "may disclose".

[127] Section 18(1)(e) repeats the language of ss. 12(1)(e) and 15(1)(e), except again that "may disclose" replaces "may collect" or "may use".

[128] The *PIPA Regulations* set out prescribed sources of public information for the purposes of ss. 12(1)(e), 15(1)(e) and 18(1)(e). Section 6 lists the following prescribed sources of public information: (a) telephone directories; (b) professional or business directories; (c) registries that the public can access and where the information was collected under legal authority; and (d) printed or electronic publications, including a magazine, book, or newspaper in printed or electronic form.

[129] *PIPA* also sets out the role of the commissioner and grants the commissioner the power to initiate investigations and make orders. As part of their general powers under s. 36, the commissioner may "initiate investigations and audits to ensure compliance with the *Act*, if the commissioner is satisfied there are reasonable grounds to believe that an organization is not complying with the *Act*", whether or not they have received a complaint: s. 36(1)(a). The commissioner may also make an order under s. 52(3), whether or not a review has been requested: s. 36(1)(b).

[130] Section 52(3) provides:

> (3) If the inquiry is into a matter not described in subsection (2), the commissioner may, by order, do one or more of the following:
>
> (a) confirm that a duty imposed under this Act has been performed or require that a duty imposed under this Act be performed;

> (b) confirm or reduce the extension of a time limit under section 31;
>
> (c) confirm, excuse or reduce a fee, or order a refund, in the appropriate circumstances;
>
> (d) confirm a decision not to correct personal information or specify how personal information is to be corrected;
>
> (e) require an organization to stop collecting, using or disclosing personal information in contravention of this Act, or confirm a decision of an organization to collect, use or disclose personal information;
>
> (f) require an organization to destroy personal information collected in contravention of this Act.

[131] The commissioner may specify any terms or conditions in an order, pursuant to s. 52(4).

[132] Once an organization receives an order, it has a duty to comply within 30 days of receipt under s. 53. However, if an application for judicial review is brought within that 30-day period, then the order will be stayed until a court orders otherwise.

B. Was the Tribunal's Interpretation of "Publicly Available" Unreasonable?

[133] There is no dispute that the impugned information in this case is "personal information" within the definition of the *Act*. Clearview also acknowledges that it did not seek consent from the individuals whose information it collected, used or disclosed. Nor is there any suggestion that Clearview gave the affected individuals notice of its activities.

[134] Rather, Clearview argues that consent was not required as the impugned information was "publicly available" such that it fell under the exceptions for collecting, using, and disclosing information without the individual's consent under *PIPA*. This argument was advanced before the tribunal by Clearview, and rejected by the Commissioner.

[135] Clearview submits that the Commissioner's conclusion that the impugned information was not "publicly available", was unreasonable.

1. Statutory Interpretation and Reasonableness Review

[136] The reasonableness standard of review was explained in *Vavilov* as follows:

> [99] A reviewing court must develop an understanding of the decision maker's reasoning process in order to determine whether the decision as a whole is reasonable. To make this determination, the reviewing court asks whether the decision bears the hallmarks of reasonableness — justification, transparency and intelligibility — and whether it is justified in relation to the relevant factual and legal constraints that bear on the decision: *Dunsmuir*, at paras. 47 and 74; *Catalyst*, at para. 13.

[137] In *Delta Air Lines Inc. v. Lukács,* 2018 SCC 2, Chief Justice McLachlin explained the obligation of the reviewing court to consider the reasons and the outcome:

> [12] ... Courts are required to pay "respectful attention to the reasons offered or which could be offered in support of a decision"… A reviewing court must refer "both to the process of articulating the reasons and to outcomes"…
>
> [citations omitted]

[138] In *Pacific Centre for Reproductive Medicine v. Medical Services Commission*, 2019 BCCA 315, at para. 44, the Court of Appeal summarized the indicia of reasonableness as follows:

> - A decision may be held to be unreasonable if it fails to account for relevant factors or is based largely on irrelevant factors.
> - A decision may also be found to be unreasonable if it is made for arbitrary reasons or reasons unrelated to the objects of the statute.
> - The outcome of an administrative decision may be rendered unreasonable by a misapprehension of evidence by the decision maker or where the court cannot be satisfied that the evidence supports facts found by the decision maker.
> - Finally, a disproportionately harsh result may render a decision unreasonable.
>
> (citing *Cooper v. British Columbia (Liquor Control and Licensing Branch)*, 2017 BCCA 451 at paras. 39–42)

[139] The guiding principles for statutory interpretation which apply to administrative decision makers[21] were explained in *Vavilov*. Administrative decision makers are

[21] For the purposes of these Reasons, I have used the word "tribunal" interchangeably with "administrative decision maker".

required to apply the substance of the "modern principle" of statutory interpretation. This principle requires that "the words of a statute must be read 'in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament'": *Vavilov*, at paras. 117-119.

[140] A court conducting reasonableness review must "assume that those who interpret the law – whether courts or administrative decision makers – will do so in a manner consistent with this principle of interpretation": *Vavilov*, at para, 118.

[141] There is no requirement for a tribunal to engage in a formalistic statutory interpretation exercise in every case. A reviewing court must recognize that the "specialized expertise and experience of administrative decision makers may sometimes lead them to rely, in interpreting a provision, on considerations that a court would not have thought to employ": *Vavilov*, at para. 119.

[142] The merits of a tribunal's interpretation of a statutory provision must be consistent with the text, context and purpose of the provision. In circumstances where the meaning of a statutory provision is disputed, "the decision maker must demonstrate in its reasons that it was alive to these essential elements": *Vavilov*, at para. 120.

[143] A tribunal cannot adopt an interpretation that it knows is inferior, even if it is plausible, simply because it is available and expedient to do so. The decision maker is obliged to "discern meaning and legislative intent, not to 'reverse-engineer' a desired outcome": *Vavilov*, at para. 121.

[144] Administrative decision makers must meaningfully account for the central issues and concerns raised by a party, but need not address every argument that is raised. The majority of the Supreme Court of Canada in *Vavilov* explained it thus:

> [122] It can happen that an administrative decision maker, in interpreting a statutory provision, fails entirely to consider a pertinent aspect of its text, context or purpose. Where such an omission is a minor aspect of the interpretive context, it is not likely to undermine the decision as a whole. It is well established that decision makers are not required "to explicitly address

> all possible shades of meaning" of a given provision: *Construction Labour Relations v. Driver Iron Inc.*, 2012 SCC 65, [2012] 3 S.C.R. 405, at para. 3. Just like judges, administrative decision makers may find it unnecessary to dwell on each and every signal of statutory intent in their reasons. In many cases, it may be necessary to touch upon only the most salient aspects of the text, context or purpose. If, however, it is clear that the administrative decision maker may well, had it considered a key element of a statutory provision's text, context or purpose, have arrived at a different result, its failure to consider that element would be indefensible, and unreasonable in the circumstances. Like other aspects of reasonableness review, omissions are not stand-alone grounds for judicial intervention: the key question is whether the omitted aspect of the analysis causes the reviewing court to lose confidence in the outcome reached by the decision maker.

[145] Where the tribunal has not explicitly considered the meaning of a relevant provision in its reasons, the court may look to the record to discern the interpretation adopted by the decision maker, and determine whether it is reasonable: *Vavilov*, at para. 123.

[146] A court conducting a reasonableness review is not permitted to perform a *de novo* analysis or try to determine the "correct" interpretation of a disputed provision. If the decision is found to be unreasonable, the reviewing court should remit the interpretative question to the original decision maker, rather than substituting its own conclusion. However, where the court concludes that the decision maker's interpretation was unreasonable and there is only one reasonable interpretation of the provision, the court may pronounce upon the interpretation of the provision, since to remit the interpretive question "would serve no useful purpose in such a case": *Vavilov*, at para. 124.

[147] I have used the above guidance in my analysis of whether the Commissioner's interpretations of "publicly available" and "reasonable purpose" were reasonable.

2. Analysis

[148] In the proceeding before the Commissioner, Clearview sought an exemption for its collection, use and disclosure of personal information without the consent of the affected individuals, on the strength of ss. 12(1)(e), 15(1)(e) and 18(1)(e) of

PIPA. Those provisions all provide an exemption if the personal information "is available to the public from a source prescribed for the purposes of this paragraph".

[149] Clearview takes issue with the Commissioner's reasons concluding that personal information published on social media websites is not publicly available within the meaning of ss. 12(1)(e), 15(1)(e) and 18(1)(e) of *PIPA*, and s. 6 of the *PIPA Regulations*.

[150] In particular, Clearview argues that the Commissioner: (1) did not "substantively engage with the purpose, text, or context" of the relevant statutory provisions and *PIPA Regulations*; and (2) did not address the arguments Clearview raised with the Privacy Commissioners. I disagree with Clearview on both fronts.

[151] That the Commissioner "substantively" engaged with the text, context and purpose of the provision, is evident when the Reasons are reviewed as whole.

[152] As noted, s. 6(1) of the *PIPA Regulations* sets out the sources of information that are available to the public which are prescribed for the purposes of paragraphs 12(1)(e), 15(1)(e), and 18(1)(e) of *PIPA*.

[153] Section 6(1) of the *PIPA Regulations* provides:

> 6(1) Subject to subsection (2), the following are sources of information available to the public, which are prescribed for the purposes of sections 12 (1) (e), 15 (1) (e) and 18 (1) (e) of the Act:
>
> (a) the name, address, telephone number and other personal information of a subscriber that appears in a telephone directory or is available through Directory Assistance if
>
> (i) the directory or the directory assistance service is available to the public, and
>
> (ii) the subscriber is permitted to refuse to have the subscriber's personal information included in the directory or made available by directory assistance;
>
> (b) personal information of an individual that appears in a professional or business directory, listing or notice that is available to the public, if the individual is permitted to refuse to have the individual's personal information included in the directory;
>
> (c) personal information appearing in a registry to which the public has a right of access, if the personal information is collected

> under the authority of an enactment, the laws of the government of Canada or a province or the bylaws of a municipality or other similar local authority in Canada;
>
> (d) personal information that appears in a printed or electronic publication that is available to the public, including a magazine, book or newspaper in printed or electronic form.
>
> [Emphasis added]

[154] The word "including" in s. 6(1)(d) indicates that the list of publicly available printed or electronic publications is non-exhaustive. Nevertheless, in interpreting this provision, the tribunal must take guidance from the examples provided, in order to understand the intent of the legislature.

[155] Paragraph 45 of the Report states as follows:

> Information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the "publicly available" exception of PIPEDA[28]. Similarly, the respective regulations of both PIPA AB and PIPA BC[29] prescribe sources of public information that include directories, registries, and publications. Social media websites and search engines are not listed as prescribed sources of publicly available information under either of these Acts. As such, collection from these sources would only be authorized with consent and only if the purposes are what a reasonable person would consider appropriate.[30]
>
> [Footnotes omitted; emphasis added]

[156] Taken on its own, the above passage could suggest that the Commissioner may not have engaged in a contextual analysis of s. 6(1)(d). More specifically, the passage does not appear to consider the implications of the word "including" which is contained in that provision, when determining if the information in this case came from the prescribed sources. However, a more holistic review of the *Decision* supports the finding that the Commissioner did not treat the items listed at s. 6(1)(d) as a closed list, when concluding that personal information published on social media websites does not constitute "publicly available" information under this provision.

[157] As noted in *Vavilov*, at para. 131, the reviewing court may look to the record to discern whether the interpretation adopted by the decision maker is reasonable.

[158] In this case, it is helpful to look at Footnote 30, which is found at the end of para. 45 of the Report. This footnote refers to an earlier investigation report of the Commissioner, entitled "*Always, sometimes, or never? Personal information & tenant screening*" ("Report P18-01"). Report P18-01 is indexed at 2018 BCIPC 13. Page 12 of Report P18-01, lists all the exceptions found under s. 6 of the *PIPA Regulations*, and then goes on to explain:

> This is a narrow set of sources of publicly available personal information. It allows collection of personal information from a professional directory such as LinkedIn, a statutory registry such as the courthouse registry, or a printed or electronic publication such as a newspaper website.
>
> ...
>
> Social media sites such as Facebook, Twitter, and Instagram or search engines such as Google are not publicly available information under PIPA. Collection from these sources would have to be with consent and be reasonable under PIPA as discussed below.

[159] It is reasonable for an administrative decision maker to utilize their institutional expertise and past decisions in interpreting their home statute: *Vavilov*, at paras. 129 -130. Furthermore, review of an administrative decision cannot be divorced from the "institutional context in which the decision was made nor from the history of the proceedings": *Vavilov*, at para. 91.

[160] The above passage from Report P18-01 indicates the Commissioner employed the modern principle of statutory interpretation and considered s. 6 as a whole and contextually. The Commissioner looked to the prescribed sources of publicly available information stipulated in s. 6(1), i.e. directories, registries, and publications. The Commissioner noted that this was a "narrow set of sources", which allowed the inclusion of LinkedIn (which constituted a professional directory), but excluded social media sites and search engines.

[161] The Commissioner's awareness and consideration of the context within which the provision was being interpreted can also be inferred from paras. 39-42 of the Report. Paragraph 39 notes the unique features of the images collected by Clearview, including the creation of biometric information in the form of vectors. Paragraph 41 notes the highly sensitive and almost permanent nature of this

information. It is followed by para. 42, which explains the connection between the nature of this personal information and any provisions exempting the need for consent:

> 41. In our view, biometric information is sensitive in almost all circumstances. It is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual. That being said, within the category of biometric information, there are degrees of sensitivity. It is our view that facial biometric information is particularly sensitive. Possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the Internet, as demonstrated in the matter at hand, or via surreptitious surveillance.
>
> 42. For these reasons, it is our view that in the absence of an applicable exception, Clearview should have obtained express opt-in consent before it collected the images of any individual in Canada.

[162] Paragraphs 61-64 of the Report, indicate that the Commissioner was aware of, and engaged in, a purposive approach to interpreting the relevant statutes:

> 61. When interpreting the Regulations, we note that as privacy legislation is considered by the courts to be quasi-constitutional,37 the rights accorded under them should be given a broad, purposive and liberal interpretation, and restrictions on those rights should be interpreted narrowly.38
>
> 62. Since the Regulations create an exemption to a core privacy protection – the requirement for collection, use and disclosure of personal information to be with consent - they should be interpreted narrowly. With this in mind, we do not accept Clearview's arguments in favour of a wider "plain language" interpretation.
>
> 63. For example, social media, from which Clearview obtained a significant proportion of the images in its database, is not specified as a "publication" in the language of the PIPEDA regulations. It is the OPC's view that social media web pages differ substantially from the sources identified in the PIPEDA regulations. As the OPC previously found in the matter of Profile Technology,[39] there are a number of key differences between online information sources such as social media, and the examples of "publications" included in 1(e):
>
> i. social media web pages contain dynamic content, with new information being added, changed or deleted in real-time; and
>
> ii. individuals exercise a level of direct control, a fundamental component of privacy protection, over their social media accounts, and over accessibility to associated content over time -for example, via privacy settings.

> 64. In addition, the OIPC BC also takes the position that social media websites are not prescribed sources of "publicly available" information, and any collection from these sources would only be authorized with consent and only if the purposes are what a reasonable person would consider appropriate.
>
> [footnotes omitted]

[163] This is further evidenced by the rejection at para. 62 of Clearview's argument "in favour of a wider 'plain language' interpretation".

[164] Paragraph 63 of the Report also demonstrates a contextual approach to understanding whether social media sites are "publicly available". Here, the Report distinguishes between social media sites and the type of "publicly available" sources listed under *PIPEDA* regulations. Two key reasons are set out for why social media should be treated differently: because social media pages are dynamic and the information on them changes constantly; and because individuals exercise a different level of control over their social media accounts, which is an important component of privacy legislation. While para. 63 only refers to *PIPEDA* as an example, it is reasonable to find that the exceptions in the *PIPEDA* regulations are analogous to those under *PIPA*. Thus, for the same reasons, the Commissioner could have reasonably found social media does not fall under the meaning of "publicly available" in *PIPA*.

[165] I turn now to the assertion that the Commissioner did not address all of the arguments Clearview raised before the Tribunal. Clearview's arguments are summarized in the Report at paras. 49-58.

[166] Clearview's assertion that the Commissioner did not adequately grapple with Clearview's arguments and the "broad definition" of publicly available, is contradicted by paras. 59-64 of the Report. Paragraph 59 expressly rejects Clearview's arguments, "based on the facts, law or available jurisprudence as outlined below". The ensuing paragraphs explain the basis for rejecting Clearview's arguments.

[167] The Commissioner did not agree with Clearview's reliance on *Lukács c. Canada (Transport, Infrastructure et Collectivités),* 2015 FCA 140. Paragraph 60 of

the Report finds that *Lukács* does not apply to *PIPA*. The passage in *Lukács* relied on by Clearview is found at para. 69 which states:

> [69] The term Publicly Available appears to me to be relatively precise and unequivocal. I interpret these words as meaning available to or accessible by the citizenry at large. This interpretation is also consistent with the apparent context and purpose of subsection 69(2) of the *Privacy Act*. That provision is located in a portion of the *Privacy Act*, entitled "Exclusions", that sets out circumstances in which the *Privacy Act*, or sections thereof, do not apply. The purpose of subsection 69(2) of the *Privacy Act* is to render the use and disclosure limitations that are contained in sections 7 and 8 of the *Privacy Act* inapplicable to Personal Information if and to the extent that the citizenry at large otherwise has the ability to access such information.

[168] The Privacy Commissioners explained why they did not consider *Lukács* applicable to *PIPA*:

> 60. It is our view that *Lukács c. Canada* is not applicable to the matter at hand, as it concerns the application of the Privacy Act, which is distinct from PIPEDA. In particular, we note that unlike in the *Privacy Act*, the meaning of "publicly available information" and what qualifies as a "publication" is specifically defined in PIPEDA, PIPA AB[35] and PIPA BC[36] by regulation (the Regulations). The Regulations thus take precedence.
>
> [Footnotes omitted][22]

[169] I find the Commissioner's treatment of *Lukács* reasonable – the case implicates a different legislative scheme that is materially different than *PIPA*.

[170] Another issue Clearview raises is that the Commissioner did not adequately consider the purpose of *PIPA*, which seeks to strike a balance between the "right of individuals to protect their personal information" one the one hand, and "the need of organizations to collect, use or disclose personal information" on the other hand.[23] Clearview argues that a purposive assessment of the *PIPA Regulations* requires a balancing of the competing interests of the individual and the organization (the "Balancing Argument"). In support, it relies on *Englander v. TELUS Communications Inc*., 2004 FCA 387, at para. 38.

---

[22] Footnote 36 specifically references s. 6 of the *PIPA Regulations*.
[23] *PIPA*, s. 2.

[171] A purposive assessment of the *PIPA Regulations* does not necessarily require the balancing exercise advocated by Clearview. That is one way that the Commissioner could have approached the issue – but it is not the only way. It was reasonably open to the Commissioner to conclude that a balancing exercise was not necessary because the balance is already achieved in the statute through the design of *PIPA* itself, which allows organizations to collect personal information with the consent of individuals, and, in some narrowly prescribed cases, without their consent.[24]

[172] Clearview's Balancing Argument also seems to give equal importance to the right of the individual and the organization. In its written submissions, Clearview argued that the rights of an organization under *PIPA* should not be restricted because they are "substantive rights in the same quasi-constitutional legislation providing rights to individuals."

[173] However, the Commissioner did not agree with this interpretation of the statute. The *Decision* gives primacy to individual rights, noting at para. 62 that the prescribed "sources of information available to the public" in the *PIPA Regulations* create an exemption to a core privacy protection – the requirement that consent be obtained if an organization wishes to collect, use and disclose personal information. This approach of giving primacy to individual rights when doing a purposive assessment of the relevant provisions is reasonable and supported by the jurisprudence.

[174] The Report notes the quasi-constitutional status of privacy legislation at para. 61, and provides case authorities in support. One of the cases referenced in the Report is *Lavigne v. Canada (Office of the Commissioner of Official Languages),* 2002 SCC 53. At para. 24 of *Lavigne*, the Court held that it is the protection of individual privacy that supports the quasi-constitutional status of privacy legislation, not the right of the organization to collect and use personal information. Building on this, the Commissioner concluded at para. 62 that "publicly available" should be

[24] Commissioner Brief of Argument, para. 97.

narrowly interpreted given that the *PIPA Regulations* create an exemption to a core privacy protection. I see nothing unreasonable about this conclusion, having regard to the purpose of the *Act*.

[175] As the Report notes at para. 65, "control is a fundamental component of privacy protection" (citing *United Foods*, at para. 19). This control is intimately connected with individual autonomy, dignity and privacy. It is thus reasonable to conclude that any exceptions to these important rights should be interpreted narrowly.

[176] Clearview takes issue with the comment at para. 65 of the Report that Clearview's interpretation "would create an extremely broad exemption that undermines the control users may otherwise maintain over their information at the source."

[177] First, it is submitted that this portion of the Report simply appeals to policy. I disagree. The impugned passage explains how Clearview's position is antithetical to one of the fundamental components of privacy protection – maintaining control over one's personal information. The full passage is set out below:

> 65. Ultimately, Clearview's assertions that publication necessarily includes "public blogs, public social media or any other public websites," taken to their natural conclusion, imply that **all** publicly accessible content on the Internet is a publication in some form or other. This would create an extremely broad exemption that undermines the control users may otherwise maintain over their information at the source. In this regard, it has been noted that control is a fundamental component of privacy protection.40
>
> [Footnotes omitted]

[178] Second, Clearview argues that this passage evidences the complete failure of the Commissioner "to recognize that the very act of publication of information on a website that is not subject to password protection or other restrictions on access is an expression of an individual exercising control over their personal information at the source".[25] Clearview argues further that interpreting "publications" to include personal information published by individuals on publicly available social media,

[25] Clearview Brief of Argument, para. 88.

blogs, or other websites is completely consistent with this principle of control over personal information. In particular, individuals who "publish personal information on social media websites without restricting access to that information (deciding, in other words, to not limit the availability of that information to the broader public) …are exercising their right to control their information".[26]

[179] This brings us back to Clearview's position that the ordinary meaning of the words "publicly available" necessitates a broad definition that should have been employed by the Commissioner. Clearview argues that if any member of the public can access something on the internet, then that information is "publicly available" within the context of *PIPA*.

[180] Clearview's interpretation is one possible way of considering the issue. However, I find that it is inferior to that adopted by the Commissioner. The Commissioner's interpretation is more attuned to the text, purpose, and context of the provision. The Commissioner took into account the particularly sensitive nature of biometric information and the impact its collection, use and disclosure can have on an individual: Report, at paras. 41 and 42.

[181] Given the highly sensitive nature of this biometric information, the Commissioner concluded that in the absence of an applicable exception, collecting such information requires explicit consent. I see nothing unreasonable in this approach adopted by the Commissioner. It is consistent with the words of the *Act* and its purpose, and is supported by earlier decisions of the Commissioner: see for example, *Canadian Tire Associate Dealers' use of facial recognition technology*, OIPC Investigation Report 23-02, 2023 BCIPC 17, 2023 CanLII Docs 2922, at 15.

[182] Clearview's argument that a person has "exhausted" their right to control personal information once it is "public",[27] also does not accord with the notion of informational privacy. This was explained by the Supreme Court of Canada in *Bykovets* as follows:

[26] Clearview Brief of Argument, paras. 87-88.
[27] Clearview Brief of Argument, paras. 91-92.

> [46] In the informational privacy context, the claimant's control over the subject matter is not determinative (*Reeves*, at para. 38). The self-determination at the heart of informational privacy means that individuals "may choose to divulge certain information for a limited purpose, or to a limited class of persons, and nonetheless retain a reasonable expectation of privacy" (*Jones*, at para. 39). Anonymity is a particularly important conception of privacy when it comes to the Internet (*Spencer*, at para. 45, citing *Westin*, at p. 32).
>
> [47] Our approach is distinct from that of the United States, where the so-called "third-party doctrine" negates a reasonable expectation of privacy "if information is possessed or known by third parties" (T. Panneck, "Incognito Mode Is in the Constitution" (2019), 104 *Minn. L. Rev.* 511, at p. 520, quoting D. J. Solove, "A Taxonomy of Privacy" (2006), 154 *U. Pa. L. Rev.* 477, at p. 528). This Court rejected the American approach at an early stage of our s. 8 jurisprudence (*R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 S.C.R. 417, at pp. 429-30, per La Forest J.).
>
> [48] The non-determinative nature of control in our analysis is particularly relevant for the Internet, which requires that users reveal subscriber information to their ISP to participate in this new public square. As we said in *Jones*, "the only way to retain control over the subject matter of the search vis-à-vis the service provider was to make no use of its services at all. That choice is not a meaningful one. …Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives" (para. 45).

[183] In a similar vein, in *United Foods,* the Court held:

> [27] It goes without saying that by appearing in public, an individual does not automatically forfeit his or her interest in retaining control over the personal information which is thereby exposed. This is especially true given the developments in technology that make it possible for personal information to be recorded with ease, distributed to an almost infinite audience, and stored indefinitely.

[184] This reasoning is consistent with previous decisions of privacy commissioners, such as *Company's re-use for millions of Canadian Facebook user profiles violated privacy law,* OPC, PIPEDA Report of Findings, #2018-002, 2018 CanLII 101599:

> [92] In the case of Facebook profiles, it is not clear, in our view, that individuals would have intended to make their information public, particularly in this case, as the Facebook profiles at issue were created at a time when Facebook was relatively new and its policies were in flux. Also, at that time, Facebook profiles were set, by default, to be indexed by search engines. However, as detailed in our PIPEDA Report of Findings #2009-008, our Office took issue with this default setting, indicating that it would not have been consistent with users' reasonable expectations and was not fully explained to users. In addition, individuals may post information on Facebook

> for a variety of reasons (for example to be found and contacted by friends), and not necessarily to disseminate information to the public at large.

[185] In my view, the Commissioner was entitled to apply his specialized knowledge and expertise to the question of how social media websites should be treated within the context of *PIPA*. In this case, the Commissioner applied a definition that he believed was consistent with the text of the statute, as well as its purpose and context. I see nothing unreasonable in the Commissioner's approach or the conclusions that he arrived at in relation to how to interpret "publicly available".

[186] I turn now to whether the Commissioner adequately addressed Clearview's *Charter* argument that its freedom of expression under s. 2(b) was engaged.

[187] Clearview submits that the plain language meaning of "publicly available" lends itself to a broad interpretation that would provide an exemption for the impugned information. However, if the decision maker disagrees and rejects the plain language meaning, this means that the language of the provision is ambiguous. In order to resolve this ambiguity, it submits that the decision maker must consider *Charter* values.

[188] Section 2(b) of the *Charter* provides as follows:

> 2. Everyone has the following fundamental freedoms:
>
> …
>
> b. freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication.
>
> …

[189] The purpose of s. 2(b) is to "promote truth, political and social participation, and self-fulfilment": *Ross v. New Brunswick School District No. 15,* [1996] 1 SCR 825, 1996 CanLII 237 (S.C.C.), at para. 59.

[190] The *Charter* argument was summarized in the Report at paras. 53, 54, and 58. The *Charter* argument is explicitly addressed in the portion of the Report dealing with Quebec's *Private Sector Act*.

[191] At para. 67, the Privacy Commissioners rejected Clearview's argument that Quebec privacy legislation implicitly includes an exemption for "publicly available" information, like *PIPEDA*, *PIPA*, and other provincial statutes. In the course of this analysis, they found that Clearview had failed to show its activities advanced one of the values underlying s. 2(b) protections.

[192] The Report concludes this part of the analysis with a footnoted reference to the Supreme Court of Canada's decision in *Irwin Toy Ltd. v. Quebec (Attorney General),* 1989 CanLII 87 (S.C.C.), [1989] 1 S.C.R. 927, at 976–977. The footnote was appended to the following observation at para. 67(v) of the Report:

> Nor does it suffice to raise a freedom of expression violation. Clearview has neither explained nor demonstrated how its activities constitute the expression of a message relating to the pursuit of truth, participation in the community or individual self-fulfillment and human flourishing.[41]
>
> [Footnote omitted]

[193] It would have been preferable for the Commissioner to have done a stand-alone analysis of the issue as it related to *PIPA*, and provided more robust reasons dealing with the *Charter* values argument, particularly in relation to ambiguity. However, I do not consider this omission to undermine the reasonableness of the reasons and outcome. As held in *Vavilov*, the reasons cannot be held to a standard of perfection.

> [91] A reviewing court must bear in mind that the written reasons given by an administrative body must not be assessed against a standard of perfection. That the reasons given for a decision do "not include all the arguments, statutory provisions, jurisprudence or other details the reviewing judge would have preferred" is not on its own a basis to set the decision aside: *Newfoundland Nurses*, at para. 16. The review of an administrative decision can be divorced neither from the institutional context in which the decision was made nor from the history of the proceedings.

[194] In this case, it was reasonable for the Commissioner not to engage with the *Charter* values argument at length because the Commissioner did not consider the provision to be ambiguous. I say this having regard to the record and reasons as a whole.

[195] The decision *Bell ExpressVu Limited Partnership v. Rex*, 2002 SCC 42 states that *Charter* values need only be considered where there is genuine ambiguity:

> 62 Statutory enactments embody legislative will. They supplement, modify or supersede the common law. More pointedly, when a statute comes into play during judicial proceedings, the courts (absent any challenge on constitutional grounds) are charged with interpreting and applying it in accordance with the sovereign intent of the legislator. In this regard, although it is sometimes suggested that "it is appropriate for courts to prefer interpretations that tend to promote those [Charter] principles and values over interpretations that do not" (Sullivan, *supra*, at p. 325), **it must be stressed that, to the extent this Court has recognized a "*Charter* values" interpretive principle, such principle can only receive application in circumstances of genuine ambiguity, i.e., where a statutory provision is subject to differing, but equally plausible, interpretations.**
>
> [emphasis added]

[196] There is nothing in the *Decision* that lends itself to the conclusion that the Commissioner found the provision to be ambiguous, let alone "genuinely" so.

[197] It is also notable that the Privacy Commissioners found at para. 67(v) of the Report that the *Charter* argument was lacking. The Privacy Commissioners found that Clearview is engaged in a for-profit commercial enterprise: Report, at para. 88. It is difficult to understand how Clearview's s. 2(b) *Charter* rights are infringed through an interpretation of "publicly available" which excludes it from collecting personal information from social media websites without consent. There is no obvious connection between the collection of data for business purposes and the ability of an organisation to express itself.

[198] There is also no similarity between this case and *United Foods.* In *United Foods*, the Court found the *Alberta PIPA* was restricting a union from expressive activities in relation to labour relations. The Supreme Court of Canada emphasized the "fundamental importance" of freedom of expression in labour disputes: *United Foods,* at para. 29. That is not the case here.

[199] Clearview' s situation is not analogous to a circumstance where *PIPA* "impede[s] the formulation and expression of views on matters of significant public interest and importance": *United Foods,* at para. 27.

[200] As held in *Vavilov*, at para. 122, even when a decision maker's statutory interpretation analysis fails to consider a relevant aspect of the text, context, or purpose, the decision may nonetheless be reasonable. The key question is "whether the omitted aspect of the analysis causes the reviewing court to lose confidence in the outcome reached by the decision maker". In this case, the omitted aspect of the analysis does not cause me to lose confidence in the outcome the Commissioner reached.

[201] I find that any omission in addressing the *Charter* argument does not undermine the fact that the Commissioner was alive to Clearview's argument, the reasonableness of the outcome, or the internal chain of reasoning in the analysis.

[202] The Commissioner concluded that, having regard to *PIPA* and the *PIPA Regulations*, social media websites are not "publicly available", even where the user has not restricted access. This is not an unreasonable conclusion based on the chain of analysis. The Commissioner's *Decision* fell within the range of reasonable outcomes.

[203] In summary, I am satisfied that the "publicly available" analysis in the *Decision* bears the hallmarks of reasonableness — justification, transparency and intelligibility. The Commissioner: (1) examined the purpose, text, and context of the relevant statutory provisions; (2) was alive to Clearview's arguments and adequately responded to them; and (3) provided an internally coherent and rational chain of analysis which was justified in relation to the facts and law.

[204] Consequently, I do not accede to this ground of judicial review.

C. Was the Tribunal's Interpretation of "Reasonable Purpose" Unreasonable?

[205] Clearview challenges the Commissioner's finding that Clearview did not have a reasonable purpose for the collection, use, and disclosure of the personal information. In so doing, it argues that the Commissioner erred because: (a) the Commissioner was required, but failed, to consider *Charter* values when determining "reasonable purpose"; and (b) the *Decision* failed to provide any reasonable basis

for rejecting Clearview's arguments regarding the purpose for which it collected, used, and disclosed personal information.

[206] The Respondents say that these arguments should be dismissed because: (1) the *Charter* values argument is a new issue raised on judicial review, and should not be considered by this Court; and (2) the Commissioner was not required to consider *Charter* values when interpreting "reasonable purpose".

[207] As noted earlier, I find that the applicable standard of review on these matters is reasonableness.

1. Should this Court Consider Clearview's *Charter* Values Argument on Judicial Review?

[208] Where an issue raised for the first time on judicial review is constitutional in nature, the reviewing court should be particularly concerned as the tribunal will be denied the opportunity to bring its expertise to bear on the issue: *C.S.,* at para. 56.

[209] All *Charter* arguments "whether based on rights, freedom or values" must be supported by a rich evidentiary record, which may be absent if the matter is heard by the reviewing court in the first instance: *Sullivan v. Canada (Attorney General)*, 2024 FCA 7, at para. 8.

[210] A reviewing court has the discretion to hear or decline to hear an argument for the first time on judicial review. In general, the court will not exercise this discretion when the applicant had an earlier opportunity to raise the issue before the administrative decision maker but did not: *Alberta (Information and Privacy Commissioner) v. Alberta Teachers' Association,* 2011 SCC 61, ("*Alberta Teachers' Association*"), at paras. 22-23.

[211] The Court of Appeal for British Columbia summarized the rationale for the general rule against admitting new issues on judicial review in *The Owners, Strata Plan VR 1120 v. Civil Resolution Tribunal,* 2022 BCCA 189, at para. 45, citing *Alberta Teachers' Association,* at paras. 23-26. They are:

a) respect for the intent of Parliament and provincial legislatures in delegating decision-making powers to administrative bodies, as opposed to the court;

b) the need to accord deference to the decisions of statutory decision-makers, particularly when a decision-maker has specialized functions or expertise; and,

c) the prejudice that arises if the court does not have an evidentiary record adequate to consider the new issue.

[212] A reviewing court must consider the above rationale when deciding whether to depart from the general rule. If any of the three factors apply, this weighs against exercising the court's discretion to hear the new issue: *The Owners, Strata Plan VR 1120*, at para. 48. As the Court of Appeal for British Columbia articulated, "In other words, if the court cannot adequately show deference to the administrative decision-maker because it cannot discern the decision-maker's views on the new issue, even by implication, this should generally lead the reviewing judge to refuse to entertain the new issue" *The Owners, Strata Plan VR 1120*, at para. 48.

[213] The parties agree that new issues should generally not be considered on judicial review: *C.S.*, at para. 56. However, they disagree as to whether the issue before me is a new issue.

[214] Clearview acknowledges that the *Charter* was not directly raised before the Commissioner in regard to interpreting "reasonable purpose". However, it submits that it should be permitted to advance this argument at this hearing because:

a) The *Charter* argument was raised in relation to the interpretation of "publicly available", such that the Commissioner had notice that the interpretation of the legislation should be informed by the *Charter*: *The Law Society of British Columbia v. Parsons*, 2016 BCCA 435, at para. 14.

b) The usual concern that the tribunal should be given an opportunity to express its views on the issue does not arise in this case. The Commissioner was given an opportunity to consider the *Charter* argument when interpreting "publicly available", but chose not to do so.

c) The tribunal is always required to consider the values underlying the *Charter* in the exercise of its discretion: *Doré*, at para. 35.

[215] I will first address points (a) and (b).

[216] I do not agree with Clearview that by raising the *Charter* issue at first instance in relation to one provision in the *Act*, it was relieved from the obligation to raise it in relation to a different statutory provision.

[217] The interpretation of "reasonable purpose" requires different considerations and engages different statutory provisions than "publicly available". The meaning of "publicly available" under s. 6 of the *PIPA Regulations* is distinct from the interpretation of the "reasonable purpose" requirement under ss. 11, 14 and 17 of *PIPA*. I find it difficult to understand how the Commissioner could be considered to have had notice of an argument that was never made. The administrative decision maker is obliged to "meaningfully" account for the central issues and concerns raised by the parties, not to divine what those arguments might be.

[218] In this case, Clearview had numerous occasions to make submissions to the Privacy Commissioners throughout the Investigation. It was also given an opportunity to respond to the Privacy Commissioners' preliminary findings and recommendations. Clearview was represented by counsel throughout. It made legal submissions to the Privacy Commissioners on the constitutional applicability of federal and provincial privacy legislation and the role of *Charter* values in interpreting the meaning of "publicly available". It failed to make any legal submissions in relation to the application of *Charter* values to the interpretation of ss. 11, 14 and 17 of *PIPA*. No explanation has been provided for this failure.

[219] Because Clearview did not make submissions on this issue at first instance, the Commissioner was denied an opportunity to consider Clearview's *Charter* values arguments in relation to the reasonable purpose provisions of the statute. I am unable to discern, let alone show proper deference to, the Commissioner's views on whether or how *Charter* values might inform the interpretation of the "reasonable purpose" test under ss. 11, 14 and 17.

[220] I conclude that as it relates to grounds (a) and (b), Clearview has provided an insufficient basis upon which this Court should exercise its discretion to consider Clearview's *Charter* values argument in relation to the interpretation of "reasonable purpose".

[221] This brings me to point (c). My comments here are isolated to the question of whether Clearview should be permitted to raise the *Charter* values argument as a new issue on judicial review on the strength of *Doré*.

[222] In my view, Clearview's reliance on *Doré* for this proposition is flawed. In the absence of explicit language affirming this, it would be incorrect to say that *Doré* stood for the principle that a party can raise *Charter* values on judicial review at first instance.

[223] The general proposition advanced by the Court in *Doré* at para. 35, must be read in conjunction with the rest of the decision. It is evident that in developing the framework on which Clearview now relies, the Court in *Doré* was contemplating a situation where *Charter* values were raised before the administrative decision maker. This is evinced at paragraph 54 where the Court states "the administrative decision-maker will generally be in the best position to consider the impact of the relevant *Charter* values on the specific facts of the case".

[224] Further, in *Doré* the reviewing court was not hearing the *Charter* arguments afresh. These arguments were initially advanced before the Disciplinary Council of the Barreau du Québec as well as on appeal to the Tribunal des professions. Before the first body, Mr. Doré argued that art. 2.03 (relied on by the Disciplinary Council to justify reprimanding Mr. Doré), violated s. 2(b) of the *Charter*: *Doré,* at para. 17. On appeal to the Tribunal, Mr. Doré did not challenge the constitutionality of art. 2.03. He did however argue that the manner in which the legislation was applied by the Disciplinary Council was unconstitutional because his comments were protected by s. 2(b) of the *Charter*: *Doré,* at para. 18. On judicial review, the Superior Court of Quebec considered the Tribunal's decision: *Doré*, at para. 20. Therefore, Mr. Doré's

argument that the Disciplinary Council's decision infringed his *Charter* rights was before both the Tribunal and the reviewing court.

[225] Thus, unlike the case at bar, the *Charter* values raised on judicial review in *Doré* were not a new issue.

[226] In *Pacific Centre for Reproductive Medicine v. Medical Services Commission*, 2019 BCCA 315 ("*Pacific Centre*"), the Court of Appeal permitted a party to argue the *Charter* issue on appeal even though the petitioner had not explicitly raised the *Charter* issue before the Commission. However, the facts of that case are also different from the case at bar. After citing the principle articulated in *Alberta Teachers' Association* that "issues should not be raised on judicial review that were not before the administrative decision maker", the Court noted that the respondent "did not seek to rely on [the petitioner's] failure to raise the issue, but focused on the closely related issue of what it says was PCRM's failure to provide a sufficient evidentiary foundation for the issue in the application record": *Pacific Centre,* at para. 87.

[227] Here, the Respondents do take issue with the Petitioner's failure to raise this issue before the Commissioner. I agree with them that it would be improper for me to consider this new argument on judicial review. Doing so raises the risk of engaging in a *de novo* analysis of the issues, based on an argument that was not made before the Commissioner.

[228] For the aforementioned reasons, I decline to exercise my discretion to permit Clearview to raise the *Charter* values argument afresh on this judicial review.

2. Was the Commissioner Required to Consider *Charter* Values when Interpreting "Reasonable Purpose"?

[229] Even if I was inclined to exercise my discretion to permit Clearview to advance the *Charter* values argument afresh on this judicial review, it would not assist Clearview. This is because I find that the Commissioner was not required to consider the *Charter* values when interpreting "reasonable purpose", both because

the decision to be made was not discretionary, and also because the language to be interpreted was not ambiguous.

[230] The *Doré* framework does not require a tribunal to consider *Charter* values every time they are assessing the application of a piece of legislation to a particular set of facts. Rather, the *Doré* framework is only engaged where an administrative decision-maker exercises discretion: *Pacific Centre for Reproductive Medicine v. Medical Services Commission*, 2019 BCCA 315, at paras. 80-81.

[231] A discretionary decision is one where "the law does not dictate a specific outcome, or where the decision-maker is given a choice of options within a statutorily imposed set of boundaries": *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 S.C.R. 817, 1999 CanLII 699, at para. 52.

[232] A discretionary decision is "somewhat flexible, generally requires weighing of multiple considerations and wherein which there may be multiple acceptable results": *Dollan v. The Owners, Strata Plan BCS 1589*, 2012 BCCA 44, at para. 13.

[233] As noted in *Pacific Centre*, *Charter* values have a very limited role to play in matters of statutory interpretation. They are used as an interpretive tool in circumstances where the legislation is genuinely ambiguous. The Court of Appeal explained it thus:

> [81] In matters of statutory interpretation, on the other hand, *Charter* values may be considered as an interpretive tool only where the legislation is ambiguous. As Justice Charron explained in *Rodgers:*
>
> > [18] … [I]t is … well settled that, in the interpretation of a statute, Charter values as an interpretative tool can *only* play a role where there is a genuine ambiguity in the legislation. In other words, where the legislation permits two different, yet equally plausible, interpretations, each of which is equally consistent with the apparent purpose of the statute, it is appropriate to prefer the interpretation that accords with Charter principles. However, where a statute is not ambiguous, the court must give effect to the clearly expressed legislative intent and not use the Charter to achieve a different result.
> >
> > [Emphasis in original]

[234] Similar to the issue raised in *Pacific Centre*, the parties here are at odds as to whether the Commissioner's decision interpreting "reasonable purpose" was a

discretionary administrative decision engaging *Doré*, or a question of statutory interpretation: *Pacific Centre*, at para. 84.

[235] However, in contrast to the conclusion reached in *Pacific Centre*, I find that the decision in this case was one of statutory interpretation, and not a discretionary decision requiring the balancing of competing values. In that regard, the situation here is similar to that in *Ontario Nurses' Association v. 10 Community Care Access Centres*, 2021, 2021 ONSC 5348, at para. 106. As in that case, the Petitioner here "is not attacking the constitutional validity of the legislation", but rather asking that it be interpreted differently: *Ontario Nurses' Association*, at para. 106.

[236] The characterization of "purposes that a reasonable person would consider appropriate under the circumstances" is not a matter of discretion. It involves an inquiry which requires the Commissioner to consider the facts before him and decide what legally constitutes an appropriate purpose. This is different than the situation in *Pacific Centre*, where the administrative decision maker "has some discretion in deciding whether the criteria are met based on the evidence before it in each particular case": *Pacific Centre*, at para. 86.

[237] In addition, I do not find the provision in question to be genuinely ambiguous.

[238] That the provision at issue is "unambiguous" is evident from its wording. Pursuant to sections 11, 14, and 17 of *PIPA*, organizations may collect, use and disclose personal information "only for purposes that a reasonable person would consider appropriate under the circumstances" and to fulfill the purposes the organization discloses under s. 10(1) or that are otherwise permitted under the *Act*. This language is clear and does not leave room for two different yet equally plausible interpretations.

[239] In conclusion, I find that the Commissioner was not required to consider *Charter* values when interpreting "reasonable purpose".

3. Is the Interpretation of Reasonable Purpose Otherwise Unreasonable?

[240] Clearview argues that the Commissioner's interpretation of "reasonable purpose" is based on "problematic" reasoning and relies on "deficient" factual conclusions.[28] For the reasons below, I find that neither of these concerns are borne out.

[241] The Report finds that Clearview's stated purpose, to "provid[e] a service to law enforcement personnel, and use by others via trial accounts", represents "the mass identification and surveillance of individuals by a private entity in the course of a commercial activity": Report, at para. 72. Based on these findings and the analytical framework established earlier in the Report, the Privacy Commissioners concluded that Clearview does not have a reasonable purpose under *PIPA*: Report, at paras. 73, 76. It was reasonable for the Commissioner to come to this conclusion.

[242] In deciding what constituted a reasonable purpose, the Commissioner in this case was required to interpret the applicable statutory language. The Report shows that the Privacy Commissioners did consider the meaning of "reasonable purpose." The Report sets out the analytical framework for determining whether a reasonable person would find Clearview's collection, use, and disclosure of personal information was for an "appropriate purpose": Report, at para. 62.

[243] Clearview's argument that the Commissioner's interpretation of "reasonable purpose" unreasonably relies upon cases concerning employee personal information, is unfounded. The Report cites past decisions to illustrate the relevant factors for determining a reasonable purpose, which are listed in footnote 43:

> The degree of sensitivity of the personal information at issue; Whether the organization's purpose represents a legitimate need / bona fide business interest; Whether the collection, use and disclosure would be effective in meeting the organization's need; Whether there are less privacy invasive means of achieving the same ends at comparable cost and with comparable benefits; and Whether the loss of privacy is proportional to the benefits

[28] Clearview's Written Submissions, paras. 107, 109, 113.

[244] It was not unreasonable for the Commissioner to rely upon past decisions for this purpose. In fact, past practices and decisions of the administrative body are relevant contextual considerations for administrative decision makers: *Vavilov,* at paras. 106-107.

[245] Clearview further argues that the *Decision* was unreasonable because the reasonable purpose analysis stemmed from the earlier conclusion that the data in question was not publicly available. I have already found that the Commissioner's interpretation of publicly available was reasonable. Given this finding, this argument cannot succeed.

[246] Clearview also argues that the *Decision* is unreasonable because it is based on a "mischaracterization" of Clearview's purpose and two "deficient" conclusions: (1) that the collection, use, and disclosure of publicly available information should be limited to the purposes for which it is published; and (2) that there is no basis to conclude that Clearview's collection, use, and disclosure of the evidence creates a risk of significant harm.

[247] During the investigation, Clearview submitted that its purpose for the collection, use, and disclosure of personal information was appropriate, given the "potential benefit of Clearview's services to law enforcement and national security": Report, at para. 85. The Commissioners rejected this characterization in the Report. Instead, they found that "Clearview's real purpose for the collection [of personal information] is a commercial for-profit enterprise": Report, at para. 88.

[248] Clearview now argues that this is a "mischaracterization" of its purpose and that because the "reasonable purpose" analysis relied on this characterization, the Decision is unreasonable.

[249] This argument seeks to attack a factual finding. In the absence of exceptional circumstances, it is inappropriate for the reviewing court to interfere with findings of fact: *Vavilov*, at para. 125. I further find that it was not unreasonable for the Commissioner to rely on that characterization of Clearview's "real purpose": Report, at para. 88.

[250] In the Report, the Commissioners found at para. 76 that Clearview did not have an appropriate purpose for:

> i. the mass and indiscriminate scraping of images from millions of individuals across Canada, including children, amongst over 3 billion images scraped world-wide;
>
> ii. the development of biometric facial recognition arrays based on these images, and the retention of this information even after the source image or link has been removed from the Internet; or
>
> iii. the subsequent use and disclosure of that information for its own commercial purposes;
>
> where such purposes:
>
> iv. are unrelated to the purposes for which the images were originally posted (for example, social media or professional networking);
>
> v. are often to the detriment of the individual (for example, investigation, potential prosecution, embarrassment, etc.); and
>
> vi. create the risk of significant harm to individuals whose images are captured by Clearview (including harms associated with misidentification or exposure to potential data breaches), where the vast majority of those individuals have never been and will never be implicated in a crime, or identified to assist in the resolution of a serious crime.

[251] Clearview submits that the decision is unreasonable because it does not provide an explanation for "why the collection, use, and disclosure of *publicly available* information would be limited to the purposes for which it was published" (emphasis added). This argument relies on a finding that the information was, in fact, publicly available. As discussed above, the Commissioner found the information was not publicly available and that finding was reasonable. Therefore, this argument does not apply.

[252] Even if this was not the case, I do not find that it was unreasonable for the Commissioner to accept and rely on this portion of the Report. In the Report, the Privacy Commissioners explicitly addressed and rejected Clearview's argument that "the purposes for which the images were originally posted and the ones for which Clearview used, collected, or disclosed them is irrelevant": Report, at para. 81. They were "not convinced" by Clearview's arguments and noted that, as a private company, it does not have authority to broadly collect personal information: Report,

at paras. 86-87. It was reasonable for the Commissioner, a decision maker with specialized expertise, to adopt these conclusions. As noted by the majority in *Vavilov*, reviewing courts should "respect administrative decision makers and their specialized expertise": at para. 75.

[253] It was also reasonable for the Commissioner to conclude that Clearview's activities "create the risk of significant harm to individuals whose images are captured".[29] This conclusion reasonably flowed from the evidence before the Commissioner, which showed: 1) Clearview had collected more than three billion images, including images of people in British Columbia and minors, 2) the "vast majority" of individuals whose personal information Clearview collected have never been and will never be implicated in a crime, and 3) Clearview marketed and sold its product to law enforcement agencies.[30] In the Report, the Privacy Commissioners also responded directly to Clearview's arguments on harm, stating at para. 89:

> Finally, we note that Clearview emphasizes the absence of harms to individuals flowing from its activities. In taking this position, Clearview fails to acknowledge: (i) the myriad of instances where false, or misapplied matches could result in reputational damage to individuals, and (ii) more fundamentally, the affront to individuals' privacy rights and broad-based harm inflicted on all members of society, who find themselves under continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images.[31]

[254] The record also included evidence and discussion regarding the risk of harm that could arise from inaccurate facial recognition results and data breaches. For example, the Report references studies that show significantly higher incidences of false positives and misidentifications of people of colour and women of colour in particular.[32] It concluded that such misidentification could lead to "significant" harms, including investigation, detention, and loss of opportunities.[33] The Privacy Commissioners rejected Clearview's assertion that their technology had a 100% accuracy rate, based on testing that it had commissioned from an independent

[29] Report, at para 76.
[30] Report, at paras. 4, 29, 76; Decision, at para.4.
[31] Report, paras. 76, 89
[32] Report, para. 95.
[33] Report, para. 95.

panel. They noted significant concerns that a variety of researchers, including the American Civil Liberties Union, raised about the testing methodology and the conclusions.[34]

[255] Regarding data breaches, the Privacy Commissioners noted that the large amount of sensitive biometric information held by Clearview "make it a high value target for malicious actors": Report, at para. 101. They rejected Clearview's argument that this was not an appropriate consideration, or that the data breach risk is present in "almost all areas of society", and that there was no likelihood of the information being stolen: Report, at para. 101. The Privacy Commissioners noted that Clearview had already publicly announced two such breaches in 2020.[35]

[256] In short, the record supported the Commissioner's conclusion regarding harm, and it was reasonable for the Commissioner to find this risk was significant.

[257] In conclusion, I find that the Commissioner's interpretation of "reasonable purpose" was reasonable. The Commissioner reasonably: (1) examined the purpose, text, and context of the relevant statutory provisions; (2) was alive to Clearview's arguments and adequately responded to them; and (3) provided an internally coherent and rational chain of analysis which was justified in relation to the facts and law. The Commissioner provided reasonable justification for the conclusions regarding reasonable purpose, and the reasons were transparent and intelligible.

IX. IS THE ORDER UNNECESSARY, UNENFORCEABLE, OR OVERBROAD?

[258] Clearview also submits that the Order is unnecessary, unenforceable, or overbroad, and should not have been made. I reject this argument on all fronts.

[259] It is useful at this juncture to reiterate the terms of the Order that are at issue:

> a. Clearview is prohibited from offering its facial recognition services that have been the subject of the investigation, and which utilize

[34] Report, para. 96.
[35] Report, para. 101

> the collection, use and disclosure of images and biometric facial arrays collected from individuals in British Columbia without their consent, to clients in British Columbia;
>
> b. Clearview shall make best efforts to cease the collection, use and disclosure of (i) images and (ii) biometric facial arrays collected from individuals in British Columbia without their consent; and
>
> c. Clearview shall make best efforts to delete the (i) images and (ii) biometric facial arrays in its possession, which were collected from individuals in British Columbia without their consent.

[260] I deal first with the question of necessity.

A. Necessity

[261] This court has held that it is a fundamental principle governing the administration of justice that unnecessary orders will not be made: *International Brotherhood of Electrical Workers, Local 213 v. Hochstein*, 2008 BCSC 1009, at para. 44. Clearview argues that, under this principle, the Order was unnecessary because it was not offering services in British Columbia at the time of the *Decision* and it offered to remain out of the province for an additional 18 months.

[262] The issue of necessity was raised by Clearview before the Commissioner, and addressed at length in the *Decision*. In relation to the first Recommendation, the Commissioner reasoned that an order was necessary as Clearview's voluntary withdrawal for 18 months did not remove the need for a binding order. He explained it thus:

> If anything, it appears Clearview is actively contemplating offering its services to Canadian and British Columbian clients in the future, albeit with some changes. Clearview has not elaborated or provided details on these proposed changes. However, it is clear that these changes will not address the heart of the issue – the collection, use and disclosure of personal information without consent, and the improper purpose this personal information is being used for.[36]

[263] The Commissioner also concluded that an order in relation to Recommendations 2 and 3 was necessary and possible to comply with. He provided the following reasons:

---

[36] Decision, para. 17.

> [18] With regard to the second and third recommendations and the argument that they are impossible to comply with, despite Clearview's argument to the contrary, its evidence and argument in the Illinois Proceeding suggests otherwise.
>
> [19] Specifically, Clearview's response to my letter of September 24, 2021 the only explanation for why the similar measures could not be implemented with regard to British Columbian information was that it "simply cannot be done."
>
> [20] Considering Clearview's public arguments in the Illinois Proceeding, I reject Clearview's bare assertion that it cannot comply and conclude that Clearview does have the means and ability to severely limit if not eliminate the collection, use, and disclosure of personal information of British Columbians. Put another way, this is not a question of cannot but rather will not.
>
> [21] In making the second and third recommendations binding, I expect Clearview to comply with those terms to the best of its ability, and at the very least, put in place the same safeguards it has with "Illinois Information" to information that originates from British Columbia and its residents.

[264] The Commissioner noted that Clearview had indicated in a court proceeding in Illinois that it was able to limit the collection and use of personal information from certain jurisdictions.[37] He quoted the following passage from Clearview's Memorandum of Law, which was filed in the Illinois Proceeding in opposition to the Plaintiff's Motion for Preliminary Injunction:

> As part of an ongoing business review commenced prior to the Motion, Clearview has recently and voluntarily changed its business practices to avoid including data from Illinois residents and to avoid transacting with non-governmental customers anywhere. Specifically, Clearview is cancelling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency. Clearview is also cancelling all accounts belonging to any entity based in Illinois. *Id.* ¶ 16. All photos in Clearview's database that were geolocated in Illinois have been blocked from being searched through Clearview's app. *Id.* ¶ 17. Going forward, Clearview has constructed a "geofence" around Illinois, and will not collect facial vectors from images that contain metadata associating them with Illinois. *Id.* ¶¶ 21–24. Clearview will not collect facial vectors from images stored on servers that are displaying Illinois IP addresses or websites with URLs containing keywords such as "Chicago" or "Illinois." *Id*. ¶ 23. Clearview is also implementing an opt-out mechanism to exclude photos from Clearview's database. *Id.* ¶ 25. Clearview's terms of use require users of the Clearview app to, among other things, agree to only use the app for law enforcement purposes and to not upload photos of Illinois residents. *Id.* ¶¶ 11, 20. To the extent that a user

[37] *Mutnick v. Clearview AI, Inc. et al*., US District Court for the Northern District of Illinois Eastern division, case number 20-cv-512 (the "Illinois Proceeding").

> nonetheless tries to upload a photo with metadata associating it with Illinois, Clearview will not initiate a search with that image or generate a face vector. *Id.* ¶ 19.
>
> …
>
> Clearview has taken steps to avoid collecting information that originates in or is associated with Illinois (the "Illinois Information"). Mulcaire Decl. ¶¶ 15–22. Specifically, Clearview will no longer run facial vectors on images from servers in Illinois and has adjusted its collection methods to avoid running facial vectors on photos with metadata associating the photo with Illinois. *Id*. ¶¶ 21–22. Clearview will also be offering Illinois residents the ability to visit Clearview's website and opt out of the use of their facial vectors or images. *Id*. ¶ 23. Clearview has blocked access to Illinois Information until the conclusion of these litigations. In the meantime, Clearview is taking measures to secure the Illinois Information. *Id*. ¶¶ 16–17.[38]

[265] The Commissioner referred to his letter of September 24, 2021, asking Clearview to explain why it could not implement similar measures for British Columbia information. He noted the following response received from Clearview on October 5, 2021:[39]

> The request and the recommendations from Privacy Commissioners were to cease the collection use and disclosure of images and biometric facial arrays collected from individuals in Canada and to delete those images. As we indicated previously, this simply cannot be done.
>
> What Clearview undertook to do in Illinois was, to the extent that there were very rough proxies available for such determination, (the meta-data of the photographs, or if the word "Chicago" appeared in the photograph) to rely on those proxies to make a limited good faith undertaking.

[266] The Commissioner was not swayed by Clearview's response. He rejected what he characterized as Clearview's "bare assertion" that it could not comply, finding "this is not a question of cannot but rather will not": *Decision,* at para. 20. He concluded that "Clearview's continued refusal to accept the finding and recommendations in the Report necessitates the issuance of a binding order": *Decision,* at para. 16.

[267] As the Commissioner held, Clearview's commitment to withdrawing from British Columbia was "voluntary and unenforceable". The fact Clearview was only willing to undertake temporary absences from the British Columbia market suggests

[38] Decision, para. 12.
[39] Decision, para. 15.

that the company intended to preserve the option of re-entering the province. Furthermore, even if Clearview refrains from marketing its services in the province, it has not committed to pausing or stopping its collection, use, and disclosure of personal information. In light of these factors, I see nothing unreasonable or even incorrect in the Commissioner's conclusion that the order was necessary.

B. Enforceability

[268] Clearview's argument regarding enforceability raises two points: (1) that the "best efforts" requirement is unenforceable; and (2) that it is impossible to determine who is a "resident" of British Columbia.

[269] According to Clearview, the "best efforts" standard is insufficiently precise and it is "impossible" to know what compliance looks like.[40] It argues that, by setting a "bare minimum", the Order does not sufficiently establish what steps Clearview must take to comply.[41]

[270] The best efforts requirement in the Order was directly related to the Illinois proceedings. The Commissioner found that in those proceedings, Clearview asserted that it had "recently and voluntarily changed its business practices" to avoid collecting data from Illinois residents. Clearview explained the steps it took to accomplish this. The Commissioner rejected Clearview's claim that it would be "impossible" to comply with the recommendations, noting that "despite Clearview's argument to the contrary, its evidence and argument in the Illinois Proceeding suggests otherwise": *Decision*, at para. 18.

[271] The Commissioner found that, even though Clearview described its measures as "rough proxies", the evidence and arguments Clearview presented in Illinois showed that it is able to "severely limit if not eliminate" the collection, use, and disclosure of personal information people in British Columbia: *Decision*, at para. 20.

[40] Clearview's Written Submissions, paras. 118, 125.
[41] Clearview's Written Submissions, para. 125.

[272] In my view, it was reasonable for the Commissioner to rely on Clearview's assertions in Illinois to scope the Order, and to reject Clearview's bald assertion that it simply could not do the same in British Columbia.

[273] Further, I do not find the Order unenforceable because of the best efforts requirement. It is not unusual for a court order to use "best efforts" language. The enforceability of such a term depends on context. In this case, Clearview knows precisely what compliance looks like, since the Order relies on Clearview's own submissions in the Illinois proceeding.

[274] In *Doucet-Boudreau v. Nova Scotia (Minister of Education)*, 2003 SCC 62, the Supreme Court of Canada considered remedies arising out of an order that the provincial government make "best efforts" to build French-language school facilities: *Doucet-Boudreau*, at para. 1. The order in *Doucet-Boudreau* required the respondent to use "best efforts to provide a homogenous French program" for certain grades by set times, and, more generally, to make "best efforts" to comply with the Order. While the order itself was not before the Supreme Court of Canada, the Court did not take issue with the "best efforts" language and, instead, found that it allowed for appropriate flexibility and allowed for unforeseen circumstances: *Doucet-Boudreau*, at paras. 13, 68.,

[275] Similarly, the Commissioner took Clearview's assertions about its own limitations into account and built flexibility into the Order by requiring the company to make "best efforts." It was reasonable for the Commissioner to set this minimum standard, informed by Clearview's claims in the Illinois proceeding that it has the ability to limit information by geography.

[276] The other aspect of Clearview's argument is that the Order is unenforceable because it is impossible to sufficiently identify personal information belonging to residents of British Columbia. There are several problems with this argument.

[277] First, the Order does not relate to "residents" of British Columbia, but rather, to "individuals in British Columbia".

[278] Second, it is disingenuous of Clearview to now say that it impossible to sufficiently identify this information, when, as the Commissioner noted, it submitted in the Illinois proceeding that it could in fact identify and restrict the collection and use of personal information that was connected to persons that were within a specific geographical location.

[279] Third, if it is indeed impossible for Clearview to sufficiently identify personal information sourced from people in British Columbia, then this is a situation of Clearview's own making. Clearview chose the method for collecting data from the internet that would inevitably capture the personal information of persons present in British Columbia. It is not an answer for Clearview to say that because the data was indiscriminately collected, any order requiring it to cease collecting data of persons present in a particular jurisdiction, is unenforceable. To that end, the Commissioner did not err in making the Order, which I consider to be enforceable.

C. Breadth

[280] This brings me to the argument that the Order, which covers information belonging to individuals "in" British Columbia rather than British Columbia "residents", is overbroad.

[281] Clearview submits that while *PIPA* protects ***residents of*** British Columbia, the Order covers personal information belonging to ***individuals in*** British Columbia, and is thus outside the statutory jurisdiction of the Commissioner. In support, Clearview relies on *Yu v. 16 Pet Food & Supplies Inc.*, 2023 BCCA 397.

[282] Beyond affirming the general principle that orders should not be overbroad, *Yu* does not assist the Petitioner. This is because *Yu* dealt with a very different factual and legal context. *Yu* concerned an appeal of an interlocutory decision to grant an injunction. It was not a judicial review of an administrative decision. The Court considered principles of overbreadth in the specific circumstances of "interlocutory and permanent injunctions made by Canadian courts to restrain defamatory or allegedly defamatory speech": *Yu*, at para. 82. The standard of review and the relevant factors the appellant Court considered in *Yu* do not apply here.

[283] In addition, the impugned order in *Yu* had a different purpose, and its overbreadth was obvious on the face. In *Yu*, the appellant made online comments "disparaging" her former employer. A chambers judge granted an interlocutory injunction requiring the appellant to "delete or remove all statements and contents" she had published online, in any forum, which referenced the employer and associated parties. The order also prevented the appellant from publishing "any statement or content" online concerning the employer and associated parties. The Court of Appeal's concerns about overbreadth related to the fact that on plain reading, the order required Ms. Yu to remove *all* posts about the named parties and restrained her from making *any* posts about them. This meant that "Ms. Yu could not retain any posts that had positive things to say about WooooF and could not make future posts to inform others that she had been sued by WooooF, was subject to an injunction not to make any statements about WooooF or perhaps offer an apology to WooooF": *Yu*, at para. 90. Importantly, the Court of Appeal did not find that the order was overbroad because the chambers judge did not have the jurisdiction to make it.

[284] Here, the question of overbreadth relates to the jurisdiction of the Commissioner to make an order that protects the personal information of persons that are physically present in British Columbia rather than just "residents" of British Columbia.

[285] It is important to recall here that *PIPA* serves to regulate the activities of organizations. This is explained in s. 2, where the stated purpose of the *Act* is to "govern the collection, use and disclosure of personal information by organizations…" In other words, the *Act* is not regulating personal information or the individuals that the personal information belongs to. It regulates the *organizations* that collect, use, and disclose that information.

[286] Section 3 of *PIPA* reinforces *PIPA's* concern with regulating the activities of organizations as they relate to the collection, use, and disclosure of personal information. Section 3 sets out "certain enumerated categories of records to which *PIPA* does not apply": *Vabuolas v. British Columbia (Information and Privacy Commissioner),* 2024 BCSC 27, at para. 15. Clearview does not argue that the

personal information it collects, uses, and discloses fits into any of the exceptions in s. 3.

[287] Further, nowhere does *PIPA* state that it only protects information belonging to individuals who are residents of British Columbia. Indeed, the very definition of "personal information" which the *Act* is designed to protect, is broad and not restricted to British Columbia residents. This is evident from the following definition set out at s. 1 of *PIPA*:

> **"personal information"** means information about an identifiable individual and includes employee personal information but does not include
>
> (a) contact information, or
>
> (b) work product information;

[288] That the legislators were alert to the issue of jurisdiction is evident from another definition in the *Act*, relating to "public body". Section 1(a) explains a public body as "a ministry of the government of British Columbia". Had the legislators wanted to, they could have similarly limited application of the *Act* to the personal information of residents of British Columbia.

[289] I also reject the argument that the Commissioner is constitutionally confined to only making orders in relation to privacy interests of British Columbia residents. First, no authority was provided to support that assertion. Second, it is not unusual for provincial legislation to apply to protect people who are "in" the province but are not residents. For example, the *Human Rights Code*, R.S.B.C. 1996, c. 210, does not narrow its application only to British Columbia residents. Indeed, it has been used to protect the rights of non-residents: see for example, *Ndamanisha v. Contemporary Security Canada*, 2011 BCHRT 63.

[290] Thus, in the absence of clear language within *PIPA* restricting its application to the personal information of only British Columbia residents, I find no legal basis to read in terminology that would do so.

[291] The wording of the Order serves to regulate the conduct of an organization that is collecting personal information of persons that have a direct link to British

Columbia – whether that link was temporary as in a visitor passing through, or more permanent, as in a resident of the province.

[292] I do not find the Order to be overbroad. Rather, it is based on Clearview's own position that it cannot identify whether individuals in photographs are British Columbia residents or people that are simply visiting British Columbia at the time the photograph was taken.

X. CONCLUSION

[293] For all the above reasons, I find that the Petitioner has failed to establish that the Tribunal erred.

[294] The Petition is dismissed.

"Shergill J."