COURT OF APPEAL FOR BRITISH COLUMBIA

Citation: *Clearview AI Inc. v. British Columbia (Information and Privacy Commissioner),* 2026 BCCA 67

Date: 20260218
Docket: CA50390

Between:

Clearview AI Inc.

Appellant
(Petitioner)

And

Information and Privacy Commissioner for British Columbia

Respondent
(Respondent)

And

Attorney General of British Columbia

Respondent

Before: The Honourable Madam Justice Horsman
The Honourable Justice Iyer
The Honourable Justice Riley

On appeal from: An order of the Supreme Court of British Columbia, dated December 18, 2024 (*Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311, Vancouver Docket S220204).

Counsel for the Appellant:	E. Cribb O. Redko
Counsel for the Respondent, Information and Privacy Commissioner for British Columbia:	D. Wu E.J.F. Plato
Counsel for the Respondent, Attorney General of British Columbia:	C. Rajotte, K.C. C. Bant
Place and Date of Hearing:	Vancouver, British Columbia October 28, 2025
Place and Date of Judgment:	Vancouver, British Columbia February 18, 2026

Written Reasons by:
The Honourable Justice Iyer

Concurred in by:
The Honourable Madam Justice Horsman
The Honourable Justice Riley

Summary:

This appeal arises from a judicial review of the British Columbia Information and Privacy Commissioner's decision that the appellant, Clearview AI Inc., contravened the Protection of Information and Privacy Act by collecting facial data of British Columbians from social media websites without their consent to use in its facial recognition business. The Commissioner prohibited Clearview from offering its facial recognition services in BC and required it to make best efforts to stop collecting facial data of British Columbians without their consent and delete the facial data of British Columbians in its possession. Clearview argues that PIPA does not apply to it as a matter of constitutional law, PIPA does not require it to obtain individual consent, and the Commissioner's order was overbroad, unnecessary, and unenforceable.

HELD: Appeal dismissed. PIPA is constitutionally applicable to Clearview because there is a real and substantial connection between its online activities and the province. It was reasonable for the Commissioner to conclude that PIPA does not exempt Clearview from obtaining individual consent because the information was not "publicly available", and Clearview did not have reasonable purpose such that consent was statutorily implied. The Order is enforceable and was a reasonable exercise of remedial discretion.

Reasons for Judgment of the Honourable Justice Iyer:

Background

Clearview's Activities

[1] The appellant, Clearview AI Inc. ("Clearview"), is a private US-based technology company that sells facial recognition software. Its search engine (or "image crawler") detects and scans (or "scrapes") human faces and associated metadata (web page title, source link, and description) from publicly accessible websites, such as YouTube, Instagram, and Facebook. Clearview's software analyzes each face using detailed measurements to produce a numerical biometric identifier (or "vector"). All facial images, associated metadata and vectors, to which I refer collectively as "facial data", are stored indefinitely on Clearview's servers. In 2017, Clearview's database contained facial data for some three billion individuals.

[2] When a Clearview client uploads a facial image of a person of interest to them, Clearview's algorithm provides them with any facial images in the Clearview database that have a matching vector and link(s) to the website(s) from which the

image(s) was scraped. The client may use the links to look for additional information associated with the face. Clearview primarily markets its services to law enforcement and other government agencies.

[3] There is no dispute that the facial data Clearview acquires, uses, and sells is "personal information" within the meaning of the *Personal Information Protection Act*, S.B.C. 2003, c. 63 [*PIPA*], and similar statutes.

[4] Clearview conducts these activities without the knowledge or consent of the individuals whose facial data it acquires. Importantly, the technology is completely indifferent to location: the scraping occurs without regard to where the individual is in the world at the time their image was posted or scraped.

Joint Investigation

[5] In early 2020, after media reports that Clearview was marketing its facial recognition services to Canadian clients, the information and privacy commissioners of British Columbia ("BC"), Alberta, Québec, and Canada commenced a joint investigation into whether Clearview was violating privacy protection laws in their jurisdictions. During the investigation, Clearview decided to withdraw from the Canadian market.

[6] The joint investigation report, issued in February 2021 ("Joint Report"), concluded that Clearview had violated protection of privacy laws in all four jurisdictions. It recommended that Clearview stop offering its facial recognition services to clients in Canada, stop collecting, using, or disclosing facial data of individuals in Canada, and delete all such stored facial data.

[7] In response to the Joint Report, Clearview confirmed it was no longer providing facial recognition services to clients in Canada. It said the other recommendations were unjustified and, in any case, it was impossible to comply with them.

Commissioner's Decision

[8] In December 2021, the BC Information and Privacy Commissioner ("Commissioner") issued a decision finding Clearview had contravened ss. 6–8, 11, 14, and 17 of *PIPA* ("Decision", indexed at *Clearview AI, Inc (Re)*, 2021 BCIPC 73). The Decision incorporated the Joint Report in its entirety and set out subsequent communications between the Commissioner and Clearview. The Commissioner had inquired about litigation against Clearview in Illinois in which Clearview had agreed to take steps to stop acquiring facial data from Illinois residents and to block client searches from examining the facial data of Illinois residents in its database. I refer to those measures as the "Illinois Measures". Clearview informed the Commissioner it could not take steps similar to the Illinois Measures in respect of persons in BC but did not say why.

[9] The Commissioner found these circumstances necessitated the following order under s. 36(1)(b) of *PIPA* ("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.

[10] Clearview applied for judicial review of the Decision. (It also sought judicial review of similar orders made by the information and privacy commissioners of Alberta and Québec: see *Clearview AI Inc v. Alberta (Information and Privacy Commissioner)*, 2025 ABKB 287 [*Clearview ABKB*] and *Clearview AI Inc. c. Commission d'accès à l'information du Québec*, 2025 QCCQ 982.)

Judicial Review

[11] In December 2024, the chambers judge dismissed Clearview's judicial review application: *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311 ("Chambers Decision"). She rejected Clearview's argument that *PIPA* could not apply to it as a matter of constitutional law, finding that its collection of facial data from individuals in BC through the internet constitutes a real and substantial connection between it and the province. The judge also rejected Clearview's arguments that it did not have to obtain consent from the individuals whose data it collected, used, and disclosed because the information was "publicly available" or had a reasonable purpose such that consent was statutorily implied. Likewise, she dismissed Clearview's submission that the Order was unnecessary, unenforceable, or overbroad.

Issues on Appeal

[12] Clearview appeals the Chambers Decision on the three grounds it advanced in the court below. The Commissioner argues that *PIPA* applies to Clearview, that his interpretation and application of *PIPA* were reasonable, and the Order is appropriate. The Attorney General of BC ("AGBC") confines her submission to the jurisdictional issue.

[13] There is no dispute that the chambers judge selected the applicable standards of review: correctness applies to the constitutional question and reasonableness applies to the other two grounds. The decision of a judicial review judge is owed no deference on appeal. The appellate court steps into the shoes of the lower court and focuses on the administrative decision: *Northern Regional Health Authority v. Horrocks*, 2021 SCC 42 at para. 10.

[14] The issues on appeal are:

a) Is *PIPA* constitutionally applicable to Clearview?

b) Did the Commissioner unreasonably interpret and apply *PIPA* in concluding that:

i) the "publicly available" exception did not apply; and

ii) Clearview did not have a reasonable purpose for its collection, use, and disclosure of personal information.

c) Is the Commissioner's remedial Order unreasonable because it includes terms that are unnecessary, unenforceable, or overbroad?

The Statutory Scheme

[15] *PIPA* balances the rights of individuals to exercise control over the collection, use, and disclosure of their personal information with the needs of organizations to collect, use, and disclose such information for legitimate purposes. Section 2 states:

> 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.

[16] To achieve this purpose, s. 6 of *PIPA* prohibits collection, use, or disclosure of an individual's personal information without their consent, unless *PIPA* authorizes otherwise.

[17] The following provisions are central to this appeal.

[18] Sections 12, 15, and 18 permit the collection, use, or disclosure of personal information without the individual's consent in specified circumstances. One of those circumstances is where the information is available to the public from a prescribed source (ss. 12(1)(e), 15(1)(e), 18(1)(e)). Section 6(1)(d) of the *PIPA* Regulations, B.C. Reg. 473/2003, prescribes one such source as:

> 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.

[19] Sections 11, 14, and 17 of *PIPA* limit the collection, use, or disclosure of personal information to "purposes that a reasonable person would consider

appropriate in the circumstances". The parties refer to this as the "reasonable person" test or exemption.

[20] *PIPA* also regulates how individuals and organizations interact with respect to personal information, including an individual's ability to access their information and provisions governing an organization's protection and retention of personal information in its custody or control. The Commissioner is empowered to administer the statute, including by conducting investigations, audits, and inquiries on his own initiative as well as in response to complaints, and may make the orders set out in s. 52.

Is *PIPA* Constitutionally Applicable to Clearview?

Applicable Legal Principles

[21] The parties agree that for the application of *PIPA* and the Order to be constitutionally permissible, Clearview's activities must have a "sufficient" or "real and substantial" connection to BC. Those terms are interchangeable. The parties also agree that the relevant governing principles were established by the Supreme Court of Canada in *Unifund Assurance Co. v. Insurance Corp. of British Columbia*, 2003 SCC 40 [*Unifund*] and recently affirmed in *Sharp v. Autorité des marchés financiers*, 2023 SCC 29. They disagree over how those principles apply here.

[22] As summarized in *Sharp* at para. 104, *Unifund* set out four propositions for determining when a provincial regulatory regime can constitutionally apply to an out-of-province entity:

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.

[23] In *Sharp*, the Court emphasized that, although it is part of a "family" of "real and substantial connection tests", what is necessary to establish a sufficient connection in this context is different from the considerations that apply in conflicts of laws situations, such as *Club Resorts Ltd. v. Van Breda*, 2012 SCC 17 [*Van Breda*]; *Sharp* at paras. 117–123.

[24] Where, as here, the question is whether a regulatory regime applies to an out-of-province entity "as a matter of prescriptive legislative jurisdiction", the court must assess the sufficiency of the connection by engaging in a contextual inquiry into the relationship between the enacting jurisdiction, the subject matter of the law, and the person sought to be regulated: *Sharp* at paras. 123, 127. As this Court clarified in *McCabe v. British Columbia (Securities Commission)*, 2016 BCCA 7 at para. 35, the question is whether there is a real and substantial connection, not whether the particular connection is the most real and substantial.

[25] With respect to order and fairness, *Sharp* clarified that "order" refers to principles of interjurisdictional comity and "fairness" refers to fairness to the out-of-province entity. Both must be applied purposively and fairly in light of the subject matter of the legislation and the type of jurisdiction being asserted: *Sharp* at para. 131.

[26] How do these principles apply here?

Clearview's Conduct Before July 2020

[27] I distinguish between Clearview's activities up to July 2020, when it ceased marketing activity in BC, and its activities from that point forward.

[28] Prior to July 2020, Clearview was marketing its services to BC-based entities, whether on a paying or trial basis. That means it was "doing business" in BC, which is a sufficient connection to BC under the *Unifund* test. Indeed, Clearview does not argue otherwise.

[29] While the Order does not specify the time period to which it applies, it is evident from the Decision that the facts on which the Order was based included Clearview's pre-July 2020 activities.

[30] Clearview argues that conduct in which it is no longer engaging cannot provide a sufficient connection to ground BC's jurisdiction:

> 35. The fact that Clearview had, *in the past*, provided trial services to various provincial entities cannot ground the permanent application of *PIPA* to Clearview, nor the Commissioner's ongoing exercise of jurisdiction over Clearview. An entity's ongoing activity within a jurisdiction is a necessary, and indeed, fundamental component of that jurisdiction's ability to exercise ongoing prescriptive authority over that entity.
>
> 36. To hold otherwise would mean that once an entity has offered its services in British Columbia, even on a temporary trial basis, it will be permanently subject to British Columbia's prescriptive jurisdiction, including well after the entity has ceased offering its services in the province. This is an untenable proposition, inconsistent with an entity's right to cease doing business in a given jurisdiction if the regulatory context changes in a manner the entity deems unfavourable.
>
> [Emphasis in original; footnote omitted.]

[31] I agree with the respondents that the fact that an entity stops operating in a jurisdiction does not mean a regulator loses jurisdiction to issue orders, including prospective orders, that are based on the entity's wrongful conduct while it was in the jurisdiction. In *Sharp*, for example, the regulator sought five-year prospective prohibitions in 2017 against out-of-province appellants who were no longer doing business in Québec, based on their involvement in an alleged "pump-and-dump" scheme affecting Québec investors during 2011–13.

[32] While it is open to Clearview to challenge the necessity of the Order based on its open-ended prospectivity, I am satisfied that, to the extent that the Order is directed at Clearview's conduct prior to July 2020, it is constitutionally applicable to Clearview.

Clearview's Conduct After July 2020

[33] The central jurisdictional dispute in this case concerns Clearview's post-July 2020 activities, when it was no longer doing business in BC. Since then, it has

continued to acquire facial data from people all over the world, including from individuals in BC, building up the databank for its facial recognition services. In 2023, the Australian Upper Tribunal noted Clearview had acquired 30 billion facial images: *Clearview AI Inc and Australian Information Commissioner*, [2023] AATA 1069 at paras. 69, 100.

[34] Does this activity establish a sufficient connection to BC under the *Unifund* test to authorize the Order? In my view, it does.

Evolution of the "Sufficient Connection" Test

[35] The development of the internet has challenged legal principles premised on physical notions of location and territoriality. For example, in *R. v. Bykovets*, 2024 SCC 6, which concerned a challenge under s. 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 [*Charter*], to a police search resulting in disclosure of the accused's IP address, the Supreme Court of Canada rejected the argument that a person has no reasonable expectation of privacy in that information. Writing for the majority, Justice Karakatsanis commented on the impact of the internet on the assumption that a search entails a physical intrusion into a private place:

> [49] Nor is the place where the search occurred detrimental to a reasonable expectation of privacy here. This factor was largely developed in the context of territorial privacy, and digital subject matter "does not fit easily within the strictures set out by the jurisprudence" (*Marakah*, at para. 27). As this Court recently remarked, "online spaces are *qualitatively* different" from physical spaces (*R. v. Ramelson*, 2022 SCC 44, at para. 49 (emphasis in original)).

[36] She also noted the vast amount of personal information now available to private corporations to use for commercial purposes:

> [75] Not only does the Internet keep an accurate permanent record, it has concentrated this mass of data in the hands of third parties, investing these third parties with immense informational power. It has given large private corporations the ability to collect vast stores of user information and to aggregate that data into sharp images of their users' online activity to determine what their users want and when they want it. In exchange, these corporations are "building possibly the most lasting, ponderous, and significant cultural artifact in the history of humankind" (Tene, at p. 1435,

> quoting J. Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (2005), at p. 6).
>
> [76] The Internet has not only allowed private corporations to track their users, but also to build profiles of their users filled with information the users never knew they were revealing. "Browsing logs, for example, may provide detailed information about users' interests. Search engines may gather records of users' search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns" (*Spencer*, at para. 46). Commentators have even suggested that companies can use the data they collect to infer "what you are going to purchase, the kind of person you are going to get into a relationship with, whether you will be good at a new job, how long you will stay at that job, and whether you'll get sick" (H. Matsumi, "Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?" (2017), 48 *Cumb. L. Rev.* 149, at p. 149).

[37] The internet's explosive growth has also affected application of the family of real and substantial connection tests. Prior to the internet, the focus was on physical connections with the jurisdiction. Courts considered factors such as the location of the head office, employees and assets, where services or products were offered, and where the impugned conduct physically occurred: see *Cook v. Parcel, Mauro, Hultin & Spaanstra*, 1997 CanLII 4091 (B.C.C.A.), 87 B.C.A.C. 97; *Marren v. Echo Bay Mines Ltd.*, 2003 BCCA 298; *Pacific International Securities Inc. v. Drake Capital Securities Inc.*, 2000 BCCA 632.

[38] In 2004, the Supreme Court of Canada considered the then-novel challenge posed by internet music downloading to music composers holding Canadian copyrights. In *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45 [*SOCAN*], a case on which Clearview relies, Justice Binnie writing for the majority described the internet as follows:

> [2] The Internet "exists", notionally, in cyberspace. It has been described as a "fascinating exercise in symbiotic anarchy"; see G. S. Takach, *Computer Law* (2nd ed. 2003), at p. 30. It is not contained by national boundaries. The Internet thus presents a particular challenge to national copyright laws, which are typically territorial in nature.

[39] Relying on *Libman v. The Queen*, 1985 CanLII 51 (SCC), [1985] 2 S.C.R. 178, a pre-internet case involving cross-border telephone communications that were

part of a fraudulent stock scheme, Binnie J. analogized internet communications to telephone communications as being "both here and there": *SOCAN* at para. 59.

[40] That is what led to the passage in *SOCAN* on which Clearview relies:

> [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.

[41] Justice Binnie found the location of the host server was not a sufficient connection because it was simply "a piece of physical equipment, serving a neutral role as a technological conduit.": *SOCAN* at paras. 106–107.

[42] Ten years later, the courts had to consider whether Google's search engine had a sufficient connection with BC to permit the trial court to issue an injunction against it: *Equustek Solutions Inc. v. Jack*, 2014 BCSC 1063, aff'd 2015 BCCA 265, aff'd 2017 SCC 34 [*Equustek*]. In *Equustek*, the chambers judge granted an injunction against Google, a non-party, prohibiting it from including websites operated by the defendants in its search results. In the underlying action, the plaintiffs alleged the defendants, through their virtual company, had used Google's search engine to pass off the plaintiff's products as their own. Google argued, in part, that the court did not have jurisdiction over it because it was not present in Canada. The injunction issued by the chambers judge was upheld by this Court and by the Supreme Court of Canada. The comments by all three levels of court on this issue are instructive.

[43] The chambers judge noted that internet businesses challenge traditional notions of jurisdiction:

> [37] E-commerce has exponentially increased the difficulty of determining whether a company is carrying on business in a particular jurisdiction; it raises the spectre of a company being found to carry on business all over the world, just as Google submits with some alarm. Kevin Meehan comments in "The Continuing Conundrum of International Internet Jurisdiction" (2008) 31 BC Int'l & Comp L Rev 345 at 349:
>
> > In the traditional analog world, it is relatively easy for courts to determine the geographical locations of the persons, objects, and

> activities relevant to a particular case. The geography of the digital world of the Internet, however, is not as easily charted. Content providers may physically reside, conduct their business, and locate their servers in a particular location, yet their content is readily accessible from anywhere in the world. Furthermore, attempts to identify the location of a particular user over the Internet have proven extremely difficult, and many Internet users compound this problem by intentionally hiding their location. Traditional principles of international jurisdiction, particularly territoriality, are poorly suited for this sort of environment of geographic anonymity. Courts have struggled to develop a satisfactory solution, yet no progress has been made toward a uniform global standard of Internet jurisdiction.
>
> [38] In short, courts have traditionally focused on locating the behaviour in issue within a particular state's borders to ensure that "the connection between a state and a dispute cannot be weak or hypothetical [so as to] cast doubt upon the legitimacy of the exercise of state power over the persons affected by the dispute" [*Van Breda* at para. 32]. Online activities, whether commercial or otherwise, are not so easily pigeonholed.
>
> [Emphasis added.]

[44] The chambers judge rejected Google's argument that its search engine is simply a passive tool permitting BC residents to search the internet as they choose, pointing to the fact that Google both anticipates searches and sells advertising linked to searches:

> [48] I conclude that Google's internet search websites are not passive information sites. As a user begins to type a few letters or a word of their query, Google anticipates the request and offers a menu of suggested potential search queries. Those offerings are based on that particular user's previous searches as well as the phrases or keywords most commonly queried by all users. As James Grimmelman writes in "The Structure of Search Engine Law" (2007-2008) 93 Iowa L Rev 1 at 10-11:
>
> > Search engines are also increasingly learning from the large volumes of query data they have accumulated. A user's history of queries can provide useful information about her probable intentions -- for example, whether she tends towards navigational or transactional queries. Similarly, search engines gain useful feedback into their own successes and failures by seeing which results users click on or by noticing long strings of searches on related terms, which may indicate that the user is having trouble finding what she's looking for.
>
> [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. Indeed, Google entered into an advertising contract with the

> defendants and advertised their products up to the hearing of this application. Google acknowledges it should not advertise for the defendants and filed an affidavit explaining its inadvertent failure to suspend the defendants' Google account prior to the hearing.
>
> [Emphasis added.]

[45] In this Court, Justice Groberman considered that, quite apart from advertising, the fact that Google's search engine reviews trillions of web pages (including those in BC) to generate search results established a sufficient connection to ground adjudicative jurisdiction:

> [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.
>
> [Emphasis added.]

[46] Both levels of court also rejected Google's argument that an injunction should not be granted because it would amount to a world-wide order. The chambers judge reasoned:

> [64] I will address here Google's submission that this analysis would give every state in the world jurisdiction over Google's search services. That may be so. But if so, it flows as a natural consequence of Google doing business on a global scale, not from a flaw in the territorial competence analysis. …

[47] In this Court, Groberman J.A. wrote:

> [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.

[48] In the Supreme Court of Canada, Google did not challenge this Court's conclusion on jurisdiction, confining its appeal to the global reach of the injunction. The majority of the Court found the reach of the injunction justified:

> [41] I agree. The problem in this case is occurring online and globally. The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates — globally. As Fenlon J. found, the majority of Datalink's sales take place outside Canada. If the injunction were restricted to Canada alone or to google.ca, as Google suggests it should have been, the remedy would be deprived of its intended ability to prevent irreparable harm. Purchasers outside Canada could easily continue purchasing from Datalink's websites, and Canadian purchasers could easily find Datalink's websites even if those websites were de-indexed on google.ca. Google would still be facilitating Datalink's breach of the court's order which had prohibited it from carrying on business on the Internet. There is no equity in ordering an interlocutory injunction which has no realistic prospect of preventing irreparable harm.
>
> [Emphasis added.]

Application of the Unifund Test in this Case

[49] Clearview submits that, under the sufficient connection test in *SOCAN*, there is no real and substantial connection between it and BC because, even if the content providers are in BC, there is no evidence about the physical location of Clearview's servers or the servers of Facebook and other social media platforms from which Clearview's image crawler mines facial data, and the end user is not in British Columbia because Clearview no longer markets here.

[50] In my view, the *SOCAN* factors have diminished relevance because of the dramatic evolution of the internet over the last 20 years. As courts have recognized, the technological advances that have led to the proliferation of companies whose business model is based on acquiring information from global internet sites have significantly reduced the importance of physical location, whether of content providers, servers, or end users. A person can upload content, and an end user can download it, from anywhere they have an internet connection. Servers do not have to be located in territorial proximity to the companies that own them, and some servers are virtual.

[51] *Sharp* directs a contextual inquiry into the relationship between the enacting jurisdiction, the subject matter of the law, and the person sought to be regulated. The context in this case is the internet as it exists today.

[52] With respect to the relationship between it and BC, Clearview argues it is entirely indifferent to location, such that its acquisition of facial data in BC is merely "incidental" to its operation. I would disagree. Clearview's image crawler searches public websites, such as Facebook, that make billions of facial images available worldwide. Clearview's success as a business depends on its ability to acquire facial data on a global scale to build the databank on which its search engine runs, and it says it is unable to exclude BC from its image crawler's data acquisition activities. That means Clearview's access to BC (and every other jurisdiction) is essential to its operation. In my view, this supports a conclusion that BC's relationship to Clearview is substantial, not incidental.

[53] The subject matter of the law in this case is protection of the right to personal privacy, a quasi-constitutional right: *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para. 19 [*UFCW Local 401*]. It is certainly no less important than the need for transnational enforcement of provincial securities laws to combat international market manipulation, which the Supreme Court of Canada took into account in finding a sufficient connection to establish regulatory jurisdiction in *Sharp*.

[54] Clearview conflates the right to personal privacy with *PIPA* when it submits that "[t]he importance of provincial legislation is not a basis to expand that legislation's reach beyond provincial borders". The right to personal privacy is not coextensive with *PIPA*; *PIPA* is simply one of many legislative and common law mechanisms through which protection of personal privacy is achieved. The importance of the public interest in protecting that fundamental right is highly relevant in the sufficient connection analysis.

[55] Clearview's position that *PIPA* is constitutionally inapplicable to it means that it, and any other company that acquires personal information on the internet using a

global search engine, would be immune from domestic privacy laws. This would significantly compromise the ability of jurisdictions such as BC to protect personal information on the internet. In light of this, I consider Clearview's relationship to the subject matter of *PIPA* also militates in favour of a sufficient connection.

[56] Clearview says that finding a sufficient connection in this case "leads inexorably to the conclusion that once Clearview's crawlers collect a *single* photograph of a *single* person in British Columbia from any server located *anywhere* in the world" *PIPA* will apply (emphasis in original). However, that is not this case.

[57] Clearview has said its search engine roams public websites on the internet collecting facial data. By 2017 it had amassed over three billion images, which increased to 30 billion by 2023. Clearview has said it does not have the ability to geographically restrict its search engine and has not said what, if any, criteria constrain its image collection activity. That is the factual basis for finding a real and substantial connection in this case.

[58] Turning to order and fairness, Clearview argues that if *PIPA* applies to it in this case, it could lead to competing exercises of regulatory regimes undermining order in the sense of economic efficiency and creating unfairness, citing *Unifund* at paras. 71–72. Clearview builds on its unfairness argument as follows:

> 59. For example, *PIPA* would apply to any company anywhere in the world that gathers any data that might constitute personal information (e.g., the location from which a user is visiting) about a voluntary visitor to its website if that visitor happens to be in British Columbia – even if the company makes no effort whatsoever to reach out to British Columbia customers, market or sell its products in British Columbia, or otherwise act in the province.
>
> 60. Or, to give an example in another legislative context, if a company anywhere in the world advertises its services or products on the internet, a consumer who views that advertisement could have a cause of action under s. 171(1) the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2 if that advertisement was perceived as deceptive within the meaning of s. 5, even if that company did not target British Columbia or offer its products or services in the province.

[59] In my view, this argument cannot succeed.

[60] First, as the AGBC submits, the rejection of the same argument in *Sharp* applies with equal force to the cross-border acquisition of facial data and protection of the right to privacy in issue here. In *Sharp*, Binnie J. wrote:

> [134] In addition, applying Quebec's securities regulatory scheme to the appellants does not offend the principle of order or the related concept of interprovincial comity. 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).
>
> [Emphasis added.]

[61] Second, as I have explained, this case is not about the "incidental touching" of a person's publicly available data. It is about a systematic acquisition of facial data regardless of jurisdiction that enables an enterprise to commercially exploit that information by disclosing it to law enforcement and other entities who are interested in connecting with an individual. A finding that *PIPA* applies in this case says nothing about the answer to the hypothetical Clearview posits with respect to the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2.

[62] I would conclude that *PIPA* constitutionally applies to Clearview.

Did the Commissioner Unreasonably Interpret and Apply *PIPA*?

The Commissioner's Decision

[63] As I have noted, the Commissioner found *PIPA* required Clearview to obtain individual consent, rejecting its arguments that the "publicly available" exemption excused it from doing so or that its purpose for collecting the information meant consent was implied. As the Decision incorporates the Joint Report without supplementing its reasoning on these issues, the Commissioner's reasoning must be gleaned from the Decision together with the Joint Report as it relates to *PIPA*.

[64] Clearview first argued that because all the information it scraped was from publicly available sources, such as blogs, social media, and other public websites, the "publicly available" exemption applied.

[65] In relation to BC, the Joint Report found that these sources are not included in the definition of "publicly available" sources of information prescribed in the *PIPA* Regulations. Read in conjunction with ss. 12(1)(e), 15(1)(e), 18(1)(e) of *PIPA*, s. 6(1)(d) of the *PIPA* Regulations permits collection, use, and disclosure of:

> 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.

[66] The Joint Report rejected Clearview's arguments that these words should be broadly construed, and their ordinary meaning includes all publicly accessible content on the internet. It described the prescribed sources as narrow, and different in character from the social media sources from which Clearview collects facial data. The Joint Report pointed to the fact that the content of social media sources is dynamic and is subject to some level of individual control: at para. 63. Referring to the quasi-constitutional status of privacy protection, the Joint Report found restrictions on privacy rights such as s. 6(1)(d) of the *PIPA* Regulations should be interpreted narrowly: at para. 61.

[67] The Joint Report also reasoned that Clearview's broad interpretation of the exemption would undermine the individual control internet users have over their personal information:

> 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.

[68] Turning to reasonable purpose, the Joint Report listed the factors courts have developed to assist in determining whether the collection, use and/or disclosure of

personal information is reasonable within the meaning of protection of privacy statutes:

> 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.

[69] The Joint Report found the information Clearview collects was extremely sensitive for three reasons: (1) facial biometric information is key to an individual's identity and unlikely to vary over time, (2) the information includes the facial data of children, and (3) the volume of information collected is enormous and indiscriminate, amounting to billions of faces: at paras. 74–75.

[70] The Joint Report characterized Clearview's purposes for collecting and using this information as providing a commercial service to law enforcement "and use by others via trial accounts": at para. 72. It acknowledged Clearview's arguments that the information it collects is "publicly available" and provides law enforcement with a quick and accurate investigative tool, that its purposes are legitimate even if they are not the same purposes the individual had when posting their image, that any detriment to the individual is caused by law enforcement not by Clearview, and that its purposes are for the benefit of the community and public interest: at paras. 80–83.

[71] The Joint Report concluded, at paras. 73–78, that Clearview did not have a reasonable purpose for four reasons, which I would paraphrase as follows:

a) Clearview's purposes for collection, use, and disclosure are unrelated to the purposes for which the person originally posted their facial image (for example, social or networking purposes).

b) Clearview did not collect the information directly from affected individuals but from third parties who themselves were unaware of its collection activities, some of whom have complained its activity was unauthorized.

c) Clearview's use and disclosure is determinantal to the individual (for example, causing embarrassment, investigation, or potential prosecution).

d) Clearview's use and disclosure creates a risk of significant harm, including misidentification or exposure to potential data breaches when "the vast majority of those individuals … will never be implicated in a crime, or identified to assist in the resolution of a serious crime".

[72] The Joint Report also raised concerns about the accuracy of Clearview's technology, its ongoing collection of facial data despite receiving cease-and-desist letters from Google, Facebook, Twitter, YouTube, and LinkedIn, and the risk of harm arising from a data breach by malicious actors.

Reasonableness Standard of Review

[73] As the applicable standard of review is reasonableness, it is useful to review the applicable principles. They derive primarily from *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, recently affirmed in *Mason v. Canada (Citizenship and Immigration)*, 2023 SCC 21. In these cases, the Supreme Court of Canada mandated a "reasons first" approach to reasonableness review.

[74] In general, reasonableness review asks whether the reasons given by the administrative decision-maker provide a transparent and intelligible justification for the result: *Mason* at para. 60. This requires the reviewing court to read the reasons holistically and contextually, being careful not to apply a standard of perfection. Context may provide part of the reasoning process that is not apparent in the reasons: *Mason* at para. 61.

[75] With respect to statutory interpretation, the reasons under review must show the decision-maker was alive to the text, context and purpose of the statutory provision, in the sense that the analysis does not cause the reviewing court "to lose confidence in the outcome reached": *Mason* at para. 69. The record may supply what the reasons do not. Further, the decision-maker may rely on its institutional expertise and its past decisions: *Mason* at paras. 70, 75.

[76] In other words, the court must ask if the reasons given by the administrative body support the outcome it reached, not if the outcome is capable of justification, whether for the reasons given by the administrative body or not.

The "Publicly Available" Exemption

[77] Clearview argues that the Commissioner's interpretation of the exemption is not reasonable because it does not have regard for the purposes of *PIPA*, its text and context, and the Commissioner did not address its *Charter* argument.

[78] Clearview relies on s. 2 of *PIPA* as establishing the statute's purpose:

> 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.

[79] Clearview submits the language of the section establishes the purpose of *PIPA* is to create a "dual rights" regime that balances the rights of individuals to protect their personal information with the rights of organizations to collect and use it. As the chambers judge noted, Clearview's interpretation gives equal importance to the interests of individuals and organizations: Chambers Decision at para. 172.

[80] Clearview refers to no authority for its interpretation of *PIPA*'s purpose.

[81] The Joint Report does not expressly discuss the purpose section of *PIPA*. In my view, it was not necessary for it to do so. The foundation of its analysis is that the well-established purpose of protection of privacy statutes is to provide individuals with some measure of control over the use of their personal information. An individual's right to control the use of their personal information is intimately connected to their individual autonomy, dignity, and privacy. The protection provided by a statute such as *PIPA* is characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society. These principles were articulated by the Supreme Court of Canada in *UFCW Local 401* at para. 19, which is referenced in the Joint Report at footnote 40. That purpose

grounds the Joint Report's statements that the statutes require organizations to obtain individual consent in order to collect, use, or disclose personal information, unless an exception applies: Joint Report at para. 37; see also para. 44. Elsewhere, the Joint Report refers to the individual rights protected by privacy laws as quasi-constitutional, such that restrictions, including the "publicly available" exception, should be interpreted narrowly: Joint Report at para. 61, citing Supreme Court of Canada authority in support of this approach.

[82] In the absence of any jurisprudential support for Clearview's alternative interpretation of *PIPA*, I consider the Commissioner's interpretation of its purpose reasonable. The fact that the exceptions in *PIPA* also acknowledge the need of organizations to use personal information for purposes that a reasonable person would consider appropriate does not result in competing "rights". As the Federal Court of Appeal said in relation to the similarly worded purpose section of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, [*PIPEDA*], the legislation does not aim to balance competing rights, it balances a need with a right: *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FCA 140 at para. 62; leave to appeal granted 2025 CanLII 54713 (SCC).

[83] Turning to text and context, s. 6(1)(d) of the *PIPA* Regulations prescribes the information for which individual consent is not required:

> 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.

[84] The Commissioner rejected Clearview's submission that s. 6(1)(d) should be read to include all information on public websites for two reasons: first, the quasi-constitutional status of privacy protection legislation means exemptions should be interpreted narrowly and second, the meaning of "publication" in the section does not encompass social media websites.

[85] Clearview challenges the Commissioner's reliance on *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, for the

proposition that exemptions to quasi-constitutional statutory privacy rights should be interpreted narrowly. It says the purpose of the federal *Privacy Act*, R.S.C. 1985, c. P-21, which is to protect individual privacy in relation to government is very different from what it says is the "dual purpose" of *PIPA*. Having rejected Clearview's characterization of *PIPA*, as having a dual purpose in the sense of creating competing rights, it follows this argument cannot succeed. As I have discussed, the Joint Report's conclusions that *PIPA* should be characterized as quasi-constitutional legislation to the extent that it protects individual privacy rights, and exceptions to such rights should be narrowly construed, are grounded in Supreme Court of Canda authority.

[86] Further, I consider the Commissioner's specific interpretation of s. 6(1)(d) to be reasonable. The word "publication" must be understood in light of the illustrative phrase "magazine, book or newspaper". Where there is a non-exhaustive list of items in a statute or other legal document, additional items added to the list through interpretation must be of the same kind: *Clearview ABKB* at para. 82, citing *R. v. J.J.*, 2022 SCC 28 at para. 55.

[87] While magazines, books, and newspapers may be in electronic form, their content is created primarily by their authors, not by the individual readers. This is unlike social media websites where users are the primary creators of content. It follows that I would reject Clearview's argument that the Decision was unreasonable because the fact that electronic publications such as newspapers post on social media makes them analogous to social media for the purposes of s. 6(1)(d). The fact that online publications provide some opportunities for readers to comment does not make the readers primary content creators.

[88] The other exemptions in s. 6(1) are also instructive:

> (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;
>
> [Emphasis added.]

[89] The Decision reasonably characterizes these as a narrow set of sources of publicly available information.

[90] It is true that the Decision does not address Clearview's *Charter* argument in relation to *PIPA*. However, to be reasonable a decision need not address every argument advanced by a party. Recourse to the *Charter* as an interpretative tool is only available if a provision is ambiguous: Chambers Decision at para. 195, citing *Bell ExpressVu Limited Partnership v. Rex,* 2002 SCC 42 at para. 62. I agree with the chambers judge's conclusion that the record and reasons as a whole show that the Commissioner considered the statute was not ambiguous.

[91] I would conclude the Commissioner's interpretation of s. 6(1)(d) of the *PIPA* Regulations as not exempting Clearview's collection, use, and disclosure of the personal information of individuals in BC was reasonable.

Reasonable Purpose

[92] As I have noted, ss. 11, 14, and 17 of *PIPA* limit the collection, use, or disclosure of personal information to "purposes that a reasonable person would consider appropriate in the circumstances". The Decision identifies the factors courts have considered in this contextual analysis.

[93] While Clearview complains that the BC decisions referenced in the Commissioner's factum all concern employee personal information, that does not

make them irrelevant in cases not involving employees. Clearview has not demonstrated that it was unreasonable for the Decision to consider the factors it did.

[94] Clearview argues the Decision mischaracterizes its purpose for collecting facial data, it effectively deems all commercial purposes unreasonable, and it relies on speculative factual assertions about the risks of harm unsupported by the record. It says these render the Decision unreasonable.

[95] I would not accede to these arguments. First, the Decision not only reasonably, but accurately, characterizes Clearview's purpose as providing a commercial service to law enforcement and to others on a trial basis. The fact that at some point Clearview discontinued offering its service to private sector clients does not make the Decision's statement of its purpose inaccurate. In the same paragraph, the Decision describes Clearview's activity as "mass identification and surveillance of individuals by a private entity in the course of a commercial activity".

[96] This is a reasonable description in light of Clearview's description of its image crawler as collecting and creating facial data globally from websites like Facebook and YouTube in order to sell facial recognition services to law enforcement for law enforcement purposes.

[97] Clearview also takes issue with para. 88 of the Joint Report:

> Although some of the information collected may have ultimately been used for law enforcement, Clearview's real purpose for the collection is a commercial for-profit enterprise and not law enforcement.

[98] This, too, is accurate. The fact that Clearview sells personal information to law enforcement does not make its purpose "law enforcement". I note Clearview also distanced itself from law enforcement, submitting that any detriment arising to individuals from subsequent prosecution was not its responsibility: Joint Report at para. 82.

[99] Second, nothing in the Decision explicitly or implicitly says all commercial purposes are unreasonable. Clearview asserts that it does without referring to the Decision.

[100] Third, while Clearview characterizes certain facts as speculative, the Decision grounds them in the information before it. Clearview's submissions on this point simply express its disagreement with the Decision without referring to any supporting evidence. For example, while the Decision refers to published reports about inaccuracies in facial recognition technology, Clearview simply asserts its technology poses no risk of harm, speculating that persons in BC "likely form a miniscule proportion" of the facial data in its database.

[101] I consider the Commissioner's conclusion that Clearview's collection of facial data was not for purposes that a reasonable person would consider appropriate in the circumstances is reasonable. He considered relevant factors and provided four reasons supporting his conclusion. I would not accede to this ground of appeal.

Is the Commissioner's Order Unreasonable Because it Includes Terms that are Unnecessary, Unenforceable, or Overbroad?

[102] It is convenient to restate the 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.

[103] Clearview argues the first term is unnecessary because it is no longer doing business in BC. However, on the record before the Commissioner, Clearview's cessation of business activities in BC was temporary, not permanent. The timing of Clearview's departure from the Canadian market suggests that it was because of the

joint investigation. As Justice Feasby noted in *Clearview ABKB*, "[t]he rule of law would not mean much if a party subject to an investigation could escape the consequences of that investigation by leaving the jurisdiction": at para. 55. In my view, the first term of the Order is reasonable.

[104] Clearview argues the second and third terms, which require it to make "best efforts", are unenforceable because they are insufficiently precise. Although Clearview acknowledges "best efforts" language may be appropriate in some cases, it says that is not so here because the Commissioner did not say that compliance with the Illinois Measures would be sufficient, or order Clearview to implement them, and the reference to "individuals" in BC as opposed to "residents" of BC is vague.

[105] I would not accede to these arguments. Orders requiring entities to use "best efforts" are routinely made to rectify noncompliance with privacy legislation and are recognized as an effective way to tailor compliance measures to the specific circumstances of the organization and the privacy issues engaged in a particular case.

[106] In the context of *Charter* remedies, the Supreme Court of Canada has endorsed the use of "best efforts" language as allowing for flexibility and respecting the institutional roles of courts and governments: *Doucet-Boudreau v. Nova Scotia (Minister of Education)*, 2003 SCC 62 at para. 68. The case on which Clearview relies was an unopposed appeal on the permissible scope of an interim preservation order made under the *Civil Forfeiture Act*, S.B.C. 2005, c. 29. The order did not use the term "best efforts" and the Court's concerns about the vagueness of the order are not analogous to the circumstances in this case.

[107] The crafting of the Order ultimately involved an exercise of remedial discretion by the Commissioner having regard to the facts, the legislation, and Clearview's arguments. The record before the Commissioner included Clearview's failure to explain why it could not take steps similar to the Illinois Measures with respect to facial data gathered from individuals in BC. In my view, it was reasonable for the Commissioner to make an order that would require Clearview to engage with

the Commissioner and satisfy him about what it could do to rectify its privacy violations.

Conclusion

[108] In my view, *PIPA* is constitutionally applicable to Clearview. It was reasonable for the Commissioner to conclude that *PIPA* does not exempt Clearview from obtaining individual consent. I also consider the Order reasonable and enforceable. I would dismiss the appeal.

"The Honourable Justice Iyer"

I AGREE:

"The Honourable Madam Justice Horsman"

I AGREE:

"The Honourable Justice Riley"