BEYOND BORDERS: BC COURT ISSUES SEMINAL RULING ON THE JURISDICTIONAL APPLICATION OF THE *PERSONAL INFORMATION PROTECTION ACT*

Posted on January 8, 2025

Categories: Insights, Publications

In a much-anticipated decision that may have ripple effects in other jurisdictions, the British Columbia Supreme Court has provided clear guidance on the application of the *Personal Information Protection Act*, SBC 2003, c 63 ("**BC PIPA**") to foreign organizations.

In *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, the Court upheld the Office of the Information and Privacy Commissioner for British Columbia's ("**OIPC**") order against Clearview AI Inc. ("**Clearview**"), a U.S.-based facial recognition company, in connection with Clearview's violations of BC PIPA.[1]

The Court's ruling establishes that BC PIPA applies to organizations outside of British Columbia ("**BC**") that have a "real and substantial connection" to BC. Although this finding appears to support a contextual analysis similar to the test applied when considering the application of the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("**PIPEDA**") to organizations outside Canada, the BC Court expressed the view that a sufficient connection can be established for the purposes of BC PIPA merely by collecting data from individuals in BC through the Internet.[2]

Background

Clearview operates a facial recognition system that scrapes publicly accessible images from social media and other online platforms, which it then converts into biometric identifiers. Clearview's business involves selling software to law enforcement agencies and private sector entities, which allows them to match faces to the images in Clearview's searchable biometric database. At the time that Clearview's activities came to the attention of Canadian privacy regulators, the company had amassed over three billion facial images, including those of persons in BC, without their consent. Clearview's own website currently claims that its database contains over 50 billion facial images collected from the Internet (an average of six per person on the planet).[3]

In 2020, the Office of the Privacy Commissioner of Canada ("**OPC**"), along with the OIPC and the privacy commissioners in Alberta and Quebec, investigated Clearview for violations of Canada's privacy laws,

culminating in a joint investigation report (the "**Joint Investigation Report**"). The Joint Investigation Report found that Clearview contravened Canadian private-sector privacy legislation and included specific compliance recommendations for Clearview.[4]

That same year, Clearview voluntarily suspended its services to Canadian users. However, the company suggested that the suspension was intended to be temporary, and Clearview continued to collect and store images of Canadians.[5]

The OIPC's Order

In 2021, the OIPC issued an order requiring Clearview to comply with the recommendations of the Joint Investigation Report. The Alberta and Quebec privacy regulators made similar orders within their own jurisdictions. Specifically, the OIPC's order required Clearview to:[6]

1. Stop offering its facial recognition services in BC;
2. Make best efforts to cease collecting, using, or disclosing images and facial recognition data of individuals in BC without their consent; and
3. Make best efforts to delete previously collected images and facial recognition data that was collected from individuals in BC without their consent.

Clearview challenged the OIPC's order, arguing that it is not subject to BC PIPA because it does not engage in business activities within BC. In particular, Clearview focused on the fact that it has no employees, offices, or servers in BC.

In the alternative, Clearview argued that the order should be quashed because: (i) the personal information collected from online sources was "available to the public" pursuant to BC PIPA and related regulations, and therefore, Clearview did not need consent to collect the information; (ii) contrary to the findings in the Joint Investigation Report, a reasonable person would consider Clearview's purpose for collecting, using and disclosing personal information to be appropriate in the circumstances; and (iii) the OIPC's order was unnecessary and unenforceable.[7]

The Court's Findings

The Extraterritorial Jurisdiction Test

In the Joint Investigation Report, the regulators took the position that the provincial privacy statutes, including BC PIPA, apply to any private sector organization that collects, uses and discloses information of individuals within the relevant province.[8] Their finding that the location of the data subjects was determinative appeared to suggest that the provincial privacy statutes have a broader reach than the federal privacy law, as the OPC

and the courts have long recognized PIPEDA as applying only if the organization has a "real and substantial connection" to Canada.[9]

However, it does not appear that the OIPC asserted this broad jurisdictional claim to the Court on judicial review. Rather, the parties agreed that the "real and substantial connection" test is the appropriate test to determine whether provincial regulatory legislation is constitutionally applicable to out of province parties.[10] This approach effectively mirrors the one used by the OPC and the Federal Court when interpreting the application of PIPEDA.[11] Accordingly, it is now clear that the application of both federal and BC privacy laws requires a contextual analysis of the organization's connection to the relevant jurisdiction(s).

Application of the Test to Clearview

The Court agreed with the OIPC that Clearview is subject to BC PIPA. The decision sets out a lengthy analysis whereby it notes that Clearview:[12]

- Provided its services to entities in BC, including BC law enforcement;
- Carried out business and marketing in BC; and
- Collected, used and disclosed information of individuals in BC.

Consideration of all these factors is consistent with the approach taken by courts and the OPC when assessing the jurisdictional application of PIPEDA to organizations outside Canada. However, the BC Court goes a step further. In obiter, the Court suggests that, even if Clearview did not market or provide its services in BC, the act of collecting, using and disclosing personal information of individuals in BC that is gathered from the Internet, alone, would create a sufficient connection to BC for BC PIPA to apply.[13]

The Court also found that the principles of order and fairness supported the application of BC PIPA to Clearview, given that:

1. Privacy issues are increasingly cross-border in nature, and (similar to securities regulation), multi-jurisdictional regulatory authority "...promotes the seamless coverage of regulatory protection and the imposition of public interest remedies across the territories affected by a single, unlawful scheme";[14] and
2. There is nothing unfair about BC PIPA applying to Clearview since it chose to enter the BC market, advertise its product to BC law enforcement agencies, and scrape data from the Internet that includes personal information of people in BC.[15]

Finally, it is worth noting that the Court in this case found that BC PIPA does not only apply to personal information about BC residents. Rather, the legislation regulates the conduct of organizations that collect

personal information of persons with a direct link to BC, whether temporary or permanent. Accordingly, the OIPC was empowered to make orders with respect to personal information about individuals in BC regardless of whether those individuals are residents or temporary visitors in the province.[16]

Other Key Findings

1. **Publicly Available Information:** The Court dismissed Clearview's claim that it did not require consent to collect, use and disclose the personal information that was scraped from public websites because such information was "publicly available." Although BC PIPA includes some exemptions to the statutory consent requirements for information available to the public from a prescribed source, the Court agreed with the OIPC that these exemptions should be interpreted narrowly. In particular, although consent is not required to collect, use and disclose "publications" that are available to the public (such as newspapers, books and magazines) this exemption does **not** apply to all content that is posted on public blogs, public social media and other public websites.[17] Again, this finding is similar to the approach taken by the OPC and the courts when interpreting the "publicly available" exemption under PIPEDA.[18]
2. **Reasonable Purpose:** The Court upheld the OIPC's determination that Clearview lacked a "reasonable purpose" for collecting, using and disclosing personal information. In particular, the Court highlighted the risks of significant harm to individuals, including the potential for inaccurate facial recognition results and data breaches.[19]
3. **Order Validity:** The Court rejected Clearview's arguments that the OIPC's order was unnecessary, overly broad or unenforceable. The Court found the order to be necessary and consistent with BC PIPA's objectives of safeguarding personal information and protecting individual rights. It also found that Clearview was capable of making "best efforts" to cease collecting BC personal information and to delete previously collected BC data, based on representations Clearview had made in a separate court proceeding in Illinois.[20]

Significance of the Ruling

This decision reinforces the existing case law that clearly indicates that privacy laws across Canada can apply to organizations outside the country or the relevant province. While this decision is not binding on courts or regulators in other provinces, it relies upon jurisprudence from the Supreme Court of Canada that would be equally applicable in other jurisdictions. Accordingly, there is a strong possibility that a similar analysis will be applied to evaluate the application of Alberta's *Personal Information Protection Act* and Quebec's *Act respecting the protection of personal information in the private sector*.

Organizations throughout Canada and worldwide should consider the application of the "real and substantial connection" test, and evaluate whether their activities are subject to, and compliant with, Canada's federal and

provincial privacy statutes. In particular, organizations outside Canada should consider the broader regulatory and legal landscape that applies to facial recognition and data scraping technology, including the narrow definitions of "publicly available" personal information in relevant Canadian statutes. Failure to do so can result in significant costs and business impact, as demonstrated in this case where the Court upheld the OIPC's orders that effectively prohibit Clearview from offering its services in BC and require the company to undergo a potentially expensive process to geofence its data collection and purge BC data.

McMillan's experienced Privacy and Data Protection team can help organizations to conduct a thorough jurisdictional analysis, and otherwise assist companies to understand their obligations under Canadian privacy laws.

--

Related bulletins:

- *Big Brother's Access Limited – Canadian Privacy Commissioners Rule Clearview AI's Facial Recognition Tool in Breach of Canadian Privacy Laws*
- *Clearview AI Ordered to Comply with Provincial Regulators' Privacy Recommendations*
- *Scraping the Surface: Global Privacy Authorities Issue Joint Statement on Data Scraping*

[1] *Clearview AI Inc. v Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311. [**Clearview v OIPC**]
[2] Clearview v OIPC at para 90.
[3] Clearview AI, "Overview", Clearview AI (date unknown), online here.
[4] Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2021), paras 111 & 118. [**Joint Investigation Report**]
[5] Clearview v OIPC, para 2.
[6] OIPC, *Order P21-08* (December 14, 2021).
[7] Clearview v OIPC, para 4.
[8] *Joint Investigation Report*, para 33.
[9] *Joint Investigation Report*, para 28.
[10] Clearview v OIPC, paras 70-75.
[11] *A.T.* v. *Globe24h.com*, 2017 FC 114; *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, at paras 54–63 and the other authorities cited therein.
[12] Clearview v OIPC, paras 76 and 81.

[13] Clearview v OIPC, paras 90-102.
[14] Clearview v. OIPC, para 105, citing *Sharp v. Autorité des marchés financiers*, 2023 SCC 29 at para 134.
[15] Clearview v. OIPC, para 107.
[16] Clearview v. OIPC, paras 289-291.
[17] Clearview v OIPC, paras 164.
[18] See, for example, Joint Investigation Report, para 45; *A.T. v. Globe24h.com*, 2017 FC 114, para 77.
[19] Clearview v OIPC, paras 257.
[20] Clearview v OIPC, paras 267, 270-273, 279 and 292.

By Lyndsay Wasser, Kristen Pennington, Robbie Grant, Gary Preteau (Articling Student)

A Cautionary Note