The extraterritorial reach of B.C.’s privacy laws: Court upholds privacy commissioner’s order against foreign AI company

March 21, 2025

Driven by the development of AI and other technologies, companies are gaining increasing ability[1] to access and extract volumes of information from various online sources across jurisdictions. The ease and far-reaching capabilities of these data extraction or “scraping” tools give companies a competitive advantage that is enticing. With this ability, however, comes responsibility, particularly where personal information is concerned and regardless of whether the company is a foreign entity.

The highly anticipated B.C. decision of *Clearview AI Inc. v. Information and Privacy Commissioner of British Columbia*, 2024 BCSC 2311[2] is a seminal ruling on the jurisdictional application of BC’s *Personal Information Protection Act*, S.B.C. 2003, c. 63 (BC PIPA) that may have ripple effects across other jurisdictions.

Background

This case stems from a U.S.-based company’s “scraping” of images of the faces of individuals using facial recognition technology, including those in British Columbia, without their consent from various public websites and online platforms, including Facebook, YouTube, Instagram, and Twitter. The company, Clearview AI Inc. (Clearview), collected these images for the purposes of providing facial recognition services to third parties such as law enforcement agencies and private sector entities, allowing them to match faces to the images contained within Clearview’s searchable biometric database. To date, Clearview’s database contains over 50 billion facial images collected across the Internet.[3]

Following a joint investigation, the Information and Privacy Commissioner of British Columbia (the Commissioner), the Office of the Privacy Commissioner of Canada, and other privacy commissioners in Alberta and Québec issued a report that recommended that Clearview cease offering its facial recognition services to clients in Canada, cease collecting, using, and disclosing personal information collected by individuals in Canada, and delete personal information collected from individuals in Canada (the Report). Clearview refused to comply with the Report’s recommendations, causing the

Commissioner to issue an order to enforce the recommendations as they apply to individuals in British Columbia (the Order).[4]

Clearview brought a petition before the British Columbia Supreme Court seeking judicial review of the Order. In particular, Clearview challenged the Order, positing that because it has no employees, offices or servers in B.C., it is not subject to BC PIPA. Alternatively, Clearview argued that the Order should be overturned because the personal information collected from online sources was "available to the public" pursuant to BC PIPA and therefore no consent was required to collect such information.

The Court's decision

The Court dismissed Clearview's application for judicial review and upheld the Commissioner's Order. The Court made a number of findings, including two that should be of particular interest to foreign and domestic companies collecting personal information from individuals online.

a) BC PIPA applies to out-of-provinces companies that have a "real and substantial" connection to B.C.

Building on the Federal Court's landmark decision in *A.T. v. Globe24h.com*, 2017 FC 114, which addressed the application of Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) to a foreign organization, the Court agreed with the Commissioner that Clearview is subject to BC PIPA. In coming to this conclusion, the Court applied the "real and substantial connection" test to determine whether provincial regulatory legislation is constitutionally applicable to foreign entities.

In applying this contextual test, the Court considered the following:

- Clearview provided services to organizations located in BC, including law enforcement agencies such as the RCMP;
- an essential part of Clearview's business is to collect, use and disclose personal information from websites, and Clearview has amassed a database of over three billion images of faces and biometric identifiers, including those of a vast number of individuals in Canada, including children; and
- Clearview carried out business and marketing in B.C.

Most notably, the Court emphasized that even if Clearview did not market or provide its services in B.C., the simple act of collecting, using and disclosing personal information of individuals in BC from the Internet would create a sufficient connection to B.C. for BC PIPA to apply to Clearview.[5]

Finally, it is worth noting the Court's commentary regarding the unique "transnational" nature of the privacy legislative sphere and the increasing significance of such quasi-constitutional laws as technology advances.[6] For example, citing the Supreme Court of Canada's reasoning in *R v. Bykovets*, 2024 SCC 6,the Court noted the immense informational power of private corporations and that the "architecture of the Internet has led to a broad, accurate, and continuously expanding permanent record without precedent in our society."[7]

b) Not all personal information on the Internet is "publicly available"

Under BC PIPA, an organization must not collect, use, or disclose personal information about an individual without consent unless a specific exemption applies.[8] One such exemption is where the personal information is available to the public.[9]

Clearview relied on the "publicly available" exemption in arguing that consent was not required to collect the images of individuals' faces from the Internet. It argued that the prescribed sources of "publicly available" information set out in the regulations under BC PIPA, which include directories, registries, and publications, ought to be interpreted broadly to include social media websites.

In issuing the Order, the Commissioner disagreed with Clearview's position, finding that exemptions to consent, a core privacy protection, should be interpreted narrowly. Building on this, the Commissioner concluded that social media websites do not fall within the meaning of "publicly available" information.

On review, the Court upheld the Commissioner's decision, noting that the Commissioner considered various contextual factors including the sensitivity of facial biometric data, the dynamic nature of social media websites, and the level of control that individuals have over their social media accounts. The Court also agreed with the Commissioner's finding that giving primacy to individual privacy rights over the need of organizations to collect, use, and disclose personal information aligns with the purpose and quasi-constitutional status of privacy legislation.

Key takeaways

The Court's decision reinforces the existing case law that makes clear that Canadian privacy laws can apply to foreign organizations and affirms how and when aspects of BC PIPA may apply to companies who collect personal information from online sources. While this decision is not binding on courts or privacy regulatory authorities outside B.C., because it relies on jurisprudence from the Supreme Court of Canada, it is likely that a similar analysis will be applied to evaluate the application of privacy laws in other jurisdictions such as Alberta and Québec.

Companies who are planning to carry out or are currently engaged in this activity should keep in mind the following considerations.

- Companies outside of Canada ought to consider the "real and substantial connection" test and evaluate whether their business activities comply with Canada's federal and provincial privacy law statutes as well as the broader regulatory landscape that applies to the use of facial recognition technology and data scraping.
- Not all information on the Internet or accessible by members of the public is "publicly available" for the purposes of the exemptions under BC PIPA. Determining whether the "publicly available" exemption applies depends on context, including the sensitivity of the information and the level of control that individuals maintain over the personal information that is exposed online.
- While the Court's decision relates to the Commissioner's interpretation of BC PIPA, companies should be aware that analogous "publicly available" exemptions

under other Canadian private sector privacy regulations may be similarly interpreted.[10]
- The collection of personal information from online sources engages additional considerations not at play in this decision, including how to obtain meaningful consent and data minimization as a guiding principle.

For more information on how our team can assist, please contact the individuals below.

Footnotes

[1] [*Clearview AI v. BC OIPC*]. Note: Clearview AI Inc. filed a notice to appeal on January 16, 2025.

[2] [*Clearview AI v. BC OIPC*]. Note: Clearview AI Inc. filed a notice to appeal on January 16, 2025.

[3] Clearview AI Inc. Overview.

[4] Order P21-08, indexed as *Clearview AI Inc.*, 2021 BCIPC 73.

[5] *Clearview AI v. BC OIPC* at paras 90-102.

[6] *Clearview AI v. BC OIPC* at paras 95, 108.

[7] *Clearview AI v. BC OIPC* at para 99.

[8] Sections 6, 7, 8.

[9] Sections 12(1)(e), 15(1)(e), 18(1)(e).

[10] *Personal Information Protection Act Regulation*, Alta Reg 366/2003; *Regulations Specifying Publicly Available Information*, SOR/2001-7.

By

Claire Feltrin, Ingrid Vanderslice

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749