Beyond BC: Court of Appeal upholds broad reach of provincial privacy laws

March 02, 2026

BC privacy commissioner's findings that facial recognition software company, Clearview AI, contravened privacy laws upheld on appeal

On Feb. 18, 2026, the Court of Appeal for British Columbia issued its decision, *Clearview AI Inc v British Columbia (Information and Privacy Commissioner)*, 2026 BCCA 67 (the BC Appeal Decision) in which it upheld the Office of the Information and Privacy Commissioner of British Columbia's (the Commissioner) decision (Order P21-08) (the OIPCBC Decision)[1] that U.S.-based Clearview AI Inc. (Clearview) had contravened BC's *Personal Information Protection Act* (PIPA) through its facial recognition tool.

This appeal follows the Supreme Court of British Columbia's highly-anticipated December 2024 decision[2], which also upheld the Commissioner's decision on judicial review, and reaffirms the following key principles of Canadian privacy law:

- **The collection of personal information of British Columbians is likely to create a real and substantial connection between a foreign organization's activities and the province, meaning that PIPA will be constitutionally applicable to that foreign organization.**
    - This is particularly the case where an organization's business model depends on the systematic collection of personal information about individuals from online sources, even where an organization has ceased doing business in BC.[3]
- **Due to the quasi-constitutional status of privacy laws, it is reasonable for privacy commissioners to narrowly interpret exemptions (such as the "publicly available" exemption) to the requirement to obtain consent from individuals for the collection, use, or disclosure of their personal information.**
    - The exemptions to consent under PIPA do **not** create a competing "dual rights" regime where the rights of individuals to the protection of their personal information ought to be balanced with the rights of organizations to collect and use personal information for reasonable purposes. As the Court notes, "the legislation does not aim to balance competing *rights*, it balances a *need* with a *right*."[4]

- **Regardless of whether an exemption to the general consent requirement applies, an organization's collection, use, and disclosure of personal information must still be for purposes that a reasonable person would consider appropriate in the circumstances.**
    - This overarching "reasonableness" requirement is viewed by Canadian privacy regulators as a critical gateway under applicable privacy laws and a legal boundary that protects individuals from inappropriate data practices of companies, separating those legitimate information management practices that organizations may undertake in compliance with the law, from those areas in which organizations cannot venture, otherwise known as "No-go zones".

Background

Clearview provided facial recognition services to third parties, such as law enforcement, other government agencies and private sector entities, allowing them to match faces to the images contained within Clearview's searchable biometric database. Clearview developed its facial recognition tool by "scraping" billions of facial images of individuals – including individuals in Canada – without their consent from various online sources, such as social media platforms.

In February 2021, following a joint investigation, the Commissioner, along with the federal, Alberta and Québec privacy commissioners, issued a report that found that Clearview had contravened Canadian privacy laws and recommended that Clearview cease offering its facial recognition services to clients in Canada, cease collecting, using, and disclosing personal information of individuals in Canada, and delete personal information of individuals in Canada (the Report)[5]. Notably, the Canadian privacy commissioners concluded in the Report that the "publicly available" exemption to the requirement to obtain an individual's consent for the collection of their personal information did not apply to Clearview's activities.

When Clearview refused to comply with the Report's recommendations, the Commissioner issued an order (the Order) to enforce the recommendations as they apply to individuals in British Columbia.

Clearview applied for judicial review of the OIPCBC Decision and similar orders made by the Alberta and Québec privacy commissioners.[6] Please see BLG bulletins *The extraterritorial reach of B.C.'s privacy laws: Court upholds privacy commissioner's order against foreign AI company* and *Alberta judgment opens the door to the legitimization of data scraping and AI model training* for more details on the judicial review decisions of the Supreme Court of British Columbia and the Court of King's Bench of Alberta.

The Appeal Court's decision

Clearview argued that PIPA could not apply to Clearview as a matter of constitutional law, and that it did not need to obtain the consent of individuals whose facial images it collected from online sources. Clearview also argued that the Order was unnecessary, unenforceable and/or overbroad.

The Court concluded that PIPA is constitutionally applicable to Clearview as there is a real and substantial connection between Clearview and BC Even though Clearview had ceased its marketing activities in B.C. in July 2020, it continued to acquire facial images of individuals in BC after that time.

The Court emphasized that when assessing whether a real and substantial connection exists, factors such as physical location of content providers, servers and end users, which were important in historical cases, are less important today due to the evolution of the internet. Rather, the Court conducted a contextual analysis of the relationship between B.C., the subject matter of PIPA, and Clearview and determined that "BC's relationship to Clearview is substantial, not incidental."[7] The key factual basis for this finding was that Clearview's services depended on its ability to collect facial images from individuals around the world to build its database, and that because it was unable to exclude BC from its scraping activities, that meant that "Clearview's access to BC (and every other jurisdiction) is essential to its operation."[8] The Court also commented on the quasi-constitutional nature of the right to personal privacy:

> "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."[9]

And further that:

> "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."[10]

Further, the Court held that the Commissioner did not unreasonably interpret and apply PIPA in concluding that: (i) the "publicly available" exemption to consent did not apply to Clearview's activities, and (ii) Clearview did not have a reasonable purpose for its collection, use, and disclosure of personal information. The Court acknowledged that while the OIPCBC Decision did not address Clearview's argument that PIPA infringed its freedom of expression under the Canadian *Charter of Rights and Freedoms* (this argument was key in the judicial review decision of the Court of King's Bench of Alberta[11]), this did not make the Commissioner's decision unreasonable.

Finally, the Court held that the Commissioner's remedial Order was reasonable and enforceable. Clearview's appeal was dismissed.

Conclusion

The British Columbia Court of Appeal's decision in this case provides a clear and forceful affirmation of the broad territorial and substantive reach of BC's PIPA.

Organizations operating in digital and data-driven environments should take careful note: the absence of a physical presence in British Columbia will not insulate a business from the application of provincial privacy laws where there is a real and substantial connection to the province.

In particular, companies whose business models rely on the large-scale collection of personal information from online sources—especially through automated scraping or AI-enabled data aggregation—face heightened regulatory scrutiny. The Court's reasons underscore that (i) consent exceptions will be interpreted narrowly, (ii) the "publicly available" exemption does not create a parallel right to collect personal information at scale, and (iii) the overarching "reasonable purposes" requirement functions as a meaningful legal boundary, prohibiting data practices that fall into regulatory "no-go zones," even where technical arguments regarding consent may be advanced.

The decision also reinforces the quasi-constitutional status of privacy rights in Canada and signals judicial deference to privacy regulators' contextual and purposive interpretations of their home statutes. For multinational organizations, this ruling confirms that global data strategies must be assessed against local privacy frameworks, and that reliance on the borderless nature of the internet will not defeat domestic enforcement efforts.

In light of this evolving jurisprudence, organizations should proactively review their data sourcing practices, AI training methodologies, consent frameworks, and cross-border compliance strategies to ensure alignment with Canadian privacy laws. The Clearview decisions collectively represent a strong statement from Canadian courts: innovative technologies and global business models must operate within clearly defined legal limits designed to protect individuals' fundamental privacy rights.

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

Footnotes

[1] *Clearview AI, Inc (Re)*, 2021 BCIPC 73.

[2] *Clearview AI Inc v Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311.

[3] See paras 27-32 of the BC Appeal Decision.

[4] See para 82 of the BC Appeal Decision.

[5] 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, PIPEDA Findings #2021-001.

[6] See *Clearview AI Inc v Alberta (Information and Privacy Commissioner)*, 2025 ABKB 287 and *Clearview AI Inc c Commission d'accès à l'information du Québec*, 2025 QCCQ 982.

[7] See para 52 of the BC Appeal Decision.

[8] See para 52 of the BC Appeal Decision.

[9] See para 54 of the BC Appeal Decision.

[10] See para 55 of the BC Appeal Decision.

[11] See *Clearview AI Inc v Alberta (Information and Privacy Commissioner)*, 2025 ABKB 287.

By

Claire Feltrin, Danielle Windt

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Private Client, Disputes, Sports & Gaming Law, Technology

---

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 800 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

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.