Cassels

Clearview AI Faces the Wrath of Canadian Privacy Commissioners in Connection with its Exploitation of Facial Recognition Technologies

Bernice Karn, Marco Ciarlariello

February 10, 2021

Introduction

On February 2, 2021 the Office of the Privacy Commissioner of Canada (OPC) and its provincial counterparts in Quebec, British Columbia, and Alberta[1] (collectively, the Offices) released a report setting out their findings following a joint investigation of the privacy implications relating to Clearview AI, Inc.'s (Clearview) exploitation of its facial recognition tool[2] (the Report). The purpose of the investigation was to determine whether Clearview's collection and exploitation of facial images and biometric identifiers using its facial recognition tool violated federal and provincial privacy laws applicable to private organizations[3] and focused on the central questions of whether: (1) Clearview obtained the requisite consent to collect, use, and disclose personal information; and (2) Clearview had an appropriate purpose[4] for the collection, use, and disclosure of such personal information.

In investigating these issues, the Offices examined a number of threshold topics, including the application and interpretation of Canadian privacy laws as they apply to private organizations located in foreign jurisdictions and the nature of what constitutes "publicly available" personal information in Canada. In this article, we focus on the Offices' examination of these topics and outline the ways in which the approach taken by the Offices may impact Canadian and foreign businesses that operate in Canada.

Clearview's Personal Information Processing Activities and the Offices' Findings

Clearview is a technology company headquartered in the United States that develops and commercializes facial recognition software. Clearview's technology collects images of faces from online sources (including social media), creates biometric identifiers for each image, and allows users of its software to compare images that they upload against those biometric identifiers to identify the source page of the image. The facial recognition data and biometric information that are collected and created by Clearview's software constitute personal information and are considered to be sensitive in nature. The Offices found that Clearview had amassed a database of more than three billion images of facial and related biometric

identifiers, including those of individuals in Canada, some of whom were children.

The Offices determined that Clearview's collection, use, and disclosure of personal information of individuals in Canada violated the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the corresponding private sector privacy statutes in Alberta,[5] British Columbia[6] and Quebec[7] on the grounds that: (1) Clearview engaged in the collection, use, and disclosure of personal information without obtaining the requisite consents; and (2) the collection, use, and disclosure of personal information by Clearview was for inappropriate purposes. In the view of the Offices, the purpose of Clearview's collection of images and creation of biometric facial recognition data was inappropriate on the grounds that Clearview's activities: (i) were unrelated to the purpose for which the images were originally posted on the internet; (ii) were to the detriment of the individuals whose images were captured; and (iii) created a risk of significant harm to the individuals.[8] In reaching this determination, the Offices made clear that, even in circumstances in which an organization has obtained the consent of the individual to collect, use, or disclose that person's personal information, the purpose of such collection, use, or disclosure must still be for a purpose that a reasonable person would consider to be appropriate, reasonable, or legitimate in the circumstances within the meaning of applicable Canadian privacy laws.[9]

Clearview objected to the Offices' findings on a number of grounds, including:

- Clearview should not be required to seek consent of the individual data subjects on the grounds that the personal information it collected was "publicly available" within the meaning of applicable Canadian privacy laws;[10]
- Clearview's purposes for collection, use, and disclosure were appropriate because the software was intended for the sole and exclusive use of law enforcement, provided benefits to public safety, and was unlikely to result in meaningful harm to the individuals; and
- the Offices do not have jurisdiction over its activities because Clearview's activities do not take place in Canada and there was no connecting factor to create a real and substantial connection to Canada.[11]

We consider each of these arguments and the Offices' responses in the analysis below.

Analysis

Use of "Publicly Available Information"

Canadian privacy laws mandate that organizations obtain the consent of the individual data subject for the collection, use, or disclosure of personal information, unless an exception applies.[12] One such exception relates to personal information that is "publicly available" as "specified" in the regulations to PIPEDA. "Publicly available" information is a narrow concept that is often misunderstood by businesses. In the

Report, the Offices clarified the scope of what constitutes "publicly available" information and offered helpful guidance on the types of information that do not fall within the "publicly available" categories.

Clearview's argument supporting its use of publicly available information without consent stems from a broad interpretation of the word "publication" included in section 1(e) of PIPEDA's *Regulations Specifying Publicly Available Information* (the Regulation)[13] (i.e., "personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information").[14] In Clearview's assessment, the interpretation of "publication" must be broad enough to capture information on public blogs, public social media, and any other public websites. It argued that a more restrictive definition would restrict the free flow of publicly available information in a manner contrary to the freedom of expression protected under the Canadian *Charter of Rights and Freedoms*.[15] Clearview further argued that benefits of protecting personal information were outweighed by the deleterious effects that such a restriction would have by stifling Clearview's freedom of expression to use such information.[16]

In response to Clearview's arguments, the Offices noted the distinction between information that is "publicly available" as provided in the Regulation and the common understanding of information that is "publicly accessible."[17] The Offices stated that information from sources such as social media and professional profiles do not fall under the "publicly available" exceptions under the Regulation because: (1) the information on such sources can be added, changed, or deleted in real-time; and (2) individuals exercise a level of direct control over their social media accounts and the accessibility of their personal information over time.[18] The Offices argued that characterizing all personal information made available on such websites and platforms as a "publication" would make the "publicly available" exception so broad that it would undermine any control that users of such platforms may have of their personal information and defeat the purpose of the privacy settings on those platforms.[19]

The Offices also rejected Clearview's argument that a narrow interpretation of "publication" was contrary to the guarantees of freedom of expression under Quebec's *Charter of Human Rights and Freedoms*[20] and the Canadian *Charter of Rights and Freedoms*. The Offices posited that privacy laws have been considered to be quasi-constitutional by Canadian courts.[21] As a result, the rights given to individuals under Canadian privacy laws must be given a broad, purposive, and liberal interpretation, exceptions to those rights should be construed narrowly, and those principles should override the concerns raised by Clearview regarding any infringement of its right to freedom of expression.

The Offices' discourse regarding the scope of the "publicly available" exception in the Regulation is helpful for businesses seeking to leverage information that is accessible online, particularly on or through social media networks. It is important to recognize that, in Canada, merely because personal information is "publicly accessible," that does not automatically mean that it is "publicly available" within the meaning of the Regulation and can be used or disclosed for any purpose without consent.

Determination of Appropriate Purposes

In making a determination as to whether a collection, use, or disclosure of personal information is for a purpose that a reasonable person would consider to be appropriate in the circumstances, the Offices are required to engage in a "balancing of interests" between an individual's right to privacy and the commercial needs of an organization.[22] The sensitivity of the personal information is a factor to be considered as part of this analysis.

In responding to the investigation, Clearview took the position that the purpose of collection was reasonable as it was only intended as a service to enable law enforcement agencies to obtain information in the course of an investigation. Any detriment to individuals resulting from law enforcement agencies' use of the Clearview technology must be imputed to those agencies, not Clearview.[23] Clearview further argued that its objectives were beneficial to the community as its software facilitates and consolidates information required for investigations, which are functions in support of public safety.[24]

The Offices found that Clearview's "mass identification and surveillance of individuals … in the course of a commercial activity" would not be considered appropriate by a reasonable person for a variety of reasons, including:

- facial biometric information is particularly sensitive given that it is key to an individual's identity;
- the information was not collected from individuals in a legal manner (i.e., with consent);
- the purposes for which the images and biometrics were used are entirely unrelated to the purposes of which the images were originally posted;
- the use of the images and biometrics would be detrimental to the individual (i.e., for investigation by law enforcement and legal prosecution);
- the practices of Clearview create a risk of significant harm to individuals whose images are captured; and
- the collection, use, and disclosure of the facial biometric data by Clearview was for its own commercial purposes and not for the public benefit.

The Offices identified a number of additional issues with respect to Clearview's facial recognition technology, including the accuracy of the technology used, compliance with the contractual terms applicable to the websites being "scraped" by Clearview's tools,[25] and the risk of harm that could arise from a breach of Clearview's security safeguards.

The positions taken by the Offices with respect to Clearview's collection, use, and disclosure of facial images and biometric information demonstrate the importance of ensuring that purposes for which personal information is processed are reasonable in the circumstances. The Offices went to great the lengths to clarify that, even where consent is obtained from the individual, an organization may still be in breach of its privacy obligations based on the manner in which it collects, uses, or discloses personal information.

Jurisdiction of the Offices over the Activities of Clearview

The Offices rejected Clearview's position that Canadian privacy laws do not apply to Clearview's activities and noted that such laws will apply to organizations located outside of Canada where a "real and substantial connection" to Canada exists.[26] In establishing that a real and substantial connection existed between Clearview and Canada, the Offices considered the following key factors:

- Clearview had marketed its services to Canadian organizations and declared Canada to be a target market in its press releases;[27]
- Clearview had at least one paying customer in Canada and had created not less than 48 accounts for organizations cross Canada through which thousands of searches were conducted;[28] and
- a substantial amount of the images that Clearview sourced were derived from individuals in Canada and the biometric vectors derived from those images were used to market to Canadian organizations.[29]

The Offices held that a physical presence in Canada is not required to establish a real and substantial connection when considering websites under PIPEDA because the operations of a website (or other similar services) involve the transmission and receipt of personal information in Canada and between Canada and (in the case of Clearview) the United States.[30] Citing Supreme Court jurisprudence on the issue,[31] the Offices reiterated the point that receipt may be no less significant a connecting factor than the point of origin in transmission of personal information.

The Offices' findings could have far reaching implications on foreign businesses doing business in Canada that neglect to operate in compliance with Canadian privacy laws. In utilizing the real and substantial connection test, the Offices are essentially enforcing the extraterritorial application of Canadian privacy laws on the basis of principles developed through case law. Although Canadian privacy statutes do not explicitly address extraterritoriality themselves, the Offices are signaling their intent to push the boundaries of their authority to ensure that the privacy rights of individuals in Canada are respected no matter where the organization handling their information is located.

Conclusion and Key Take-aways

Clearview ultimately voluntarily withdrew from the Canadian market. However, during the process of the investigation by the Offices, Clearview had taken the position that it disagreed with the Offices' conclusions and had not committed to following the Offices' recommendations.[32] What can other organizations learn from this? In our view, the following are key points to remember:

- Merely because information is available in the public domain does not mean that it can be collected, used or disclosed for any purpose without consent or that no privacy obligations apply to it. Organizations must carefully assess the origins of such information and determine whether there is

an applicable exception to the consent requirement. Failing to do so may mean it cannot be collected, used or disclosed for the intended purpose.

- Even if a consent exception applies to public domain information, organizations must collect, use and disclose personal information for purposes that a reasonable person would consider to be appropriate in the circumstances. This is an overarching principle that applies in all cases.
- Organizations located outside of Canada may be faced with privacy investigations if they are collecting, using or disclosing personal information about individuals located in Canada. As Canadian privacy laws evolve, we may well see order making authority that could have extraterritorial impact in the future.
- Privacy regulators in Canada see privacy rights as quasi-constitutional in nature. This means that they will interpret rights in a liberal manner while reading exceptions narrowly. Organizations need to be cognizant of this when developing policies and practices – i.e., it will always be advisable to err on the side of the individual's privacy right, rather than trying to take an expansive view of any available limitation or exception.
- Lastly, the federal and provincial privacy commissioners often work together on investigations, and organizations should be prepared for that possibility. While PIPEDA has been designed to permit intraprovincial handling of personal information to be regulated by the provinces that have privacy laws that have been declared as "substantially similar" to PIPEDA, from the Clearview investigation it is clear that both levels of government were taking jurisdiction in the matter, even though the information clearly was crossing provincial and national borders.

---

[1] The Commission d'accès à l'information du Québec (CAI), the Information and Privacy Commissioner for British Columbia, and the Information and Privacy Commissioner of Alberta, respectively.

[2] *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 Report of Findings #2021-001.

[3] *Personal Information Protection and Electronic Documents Act.*

[4] The term "appropriate purpose" from PIPEDA is used inclusively in the Report by the Offices to also signify "reasonable purpose" under PIPA AB and PIPA BC and "legitimate need" under Quebec's Private Sector Act.

[5] *Personal Information Protection Act,* S.O.A., 2003, c. P-6.5, s. 11, 14, and 17. (PIPA AB).

[6] *Personal Information Protection Act*, S.B.C. 2003, c. 63, s. 6-8. (PIPA BC).

[7] *An Act Respecting the Protection of Personal Information in the Private Sector*, p. 39.1, section 6 and 12-14. (Quebec's Private Sector Act).

[8] Report at Introduction.

[9] PIPEDA s. 5(3), PIPA BC ss. 11, 14 and 17, PIPA AB ss. 11, 16 and 19 and Quebec's Private Sector Act s. 4.

[10] Report at 16.

[11] Report at 25.

[12] PIPEDA ss. 5(1), 6.1 and 7 as well as principle 4.3 of Schedule 1, PIPA AB s. 7, PIPA BC sections 6-8, Quebec's Private Sector Act sections 6 and 12-14.

[13] *Regulations Specifying Publicly Available Information* — Can. Reg. 2001-7 (*Personal Information Protection and Electronic Documents Act*). SOR/2001-7, s. 1.

[14] Clearview made similar arguments based on the definitions of publicly available information under the regulations to AB PIPA and BC PIPA as well.

[15] *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].

[16] Report at 53-54.

[17] Report at 44.

[18] Report at 63.

[19] Report at 65.

[20] *Charter of Human Rights and Freedoms*, CQLR c C-12.

[21] Report at 61.

[22] Report at 69.

[23] Report at 82.

[24] Report at 83.

[25] The Offices noted that Google, Facebook, Twitter, YouTube and LinkedIn each sent Clearview cease and desist letters in connection with Clearview's practices of collecting personal information from their platforms in violation of their terms of service.

[26] Report at 28. *Lawson v. Accusearch Inc.*, 2007 FC 125, paras. 38-51; *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 FCR 310, paras 50-64, citing *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, [2004] 2 SCR.

[27] Report at 29(i).

[28] Report at 29(ii).

[29] Report at 30(ii).

[30] Report at 31. *A.T. v. Globe24h.com* at para 54.

[31] *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, [2004] 2 SCR 427 at para 59.

[32] Report at 113-117.
