Commissariat à la protection de la vie privée du Canada | Office of the Privacy Commissioner of Canada

Commission d'accès à l'information du Québec

OIPC Office of the Information & Privacy Commissioner for British Columbia

Office of the Information and Privacy Commissioner of Alberta

REPORT OF FINDINGS

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

OPC PIPEDA-039525/CAI QC-1023158/OIPC BC P20- 81997/OIPC AB-015017

Joint Investigation by the Privacy Commissioner of Canada (OPC), the Commission d'accès à l'information du Québec (CAI), the Information and Privacy Commissioner for British Columbia (OIPC BC), and the Information and Privacy Commissioner of Alberta (OIPC AB) into Clearview AI, Inc.'s compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the *Act Respecting the Protection of Personal Information in the Private Sector*, the *Act to Establish a Legal Framework for Information Technology* (LCCJTI), the *Personal Information Protection Act* (PIPA BC), and the *Personal Information Protection Act* (PIPA AB)

Contents

Overview

The Privacy Commissioner of Canada (OPC), the Commission d'accès à l'information du Québec (CAI), the Information and Privacy Commissioner for British Columbia (OIPC BC), and the Information and Privacy Commissioner of Alberta (OIPC AB), collectively referred to as "the Offices", commenced a joint investigation[1] to examine whether Clearview AI, Inc.'s ("Clearview") collection, use and disclosure of the personal information by means of its facial recognition tool complied with federal and provincial privacy laws applicable to the private sector.

Specifically, the Offices sought to determine whether Clearview:

i. obtained requisite consent to collect, use and disclose personal information; and
ii. collected, used and disclosed personal information for an appropriate purpose[2].

Additionally, the CAI sought to determine whether Clearview had:

iii. Reported the creation of a database of biometric characteristics or measurements.

Clearview's facial recognition tool functions in four key sequential steps - Clearview:

i. **"scrapes" images** of faces and associated data from publicly accessible online sources (including social media), and stores that information in its database;
ii. **creates biometric identifiers** in the form of numerical representations for each image;
iii. **allows users to upload an image,** which is then assessed against those biometric identifiers and matched to images in its database; and
iv. **provides a list of results**, containing all matching images and metadata. If a user clicks on any of these results, they are directed to the original source page of the image.

Through this process, Clearview amassed a database of over three billion images of faces and corresponding biometric identifiers, including those of a vast number of individuals in Canada, including children.

Clearview asserted that the tool is intended for use by law enforcement,[3] for legitimate law enforcement and investigative purposes. A variety of organizations, including private sector entities, used this service via a free-trial service.

[1] Throughout this report the terms "we" and "our" are used frequently. When used outside of the context of a quoted document, these terms refer to the collective of the OPC, CAI, OIPC BC and OIPC AB.

[2] Throughout this report, the term "appropriate purpose" will be considered inclusive of "reasonable purpose" under PIPA AB and PIPA BC and "legitimate need" under *Quebec's Private Sector Act*.

[3] While Clearview indicated that the service was initially for law enforcement and security companies, at the time of this report, per Clearview's terms of service, only government agencies can create an account.

Biometric information is considered sensitive, in almost all circumstances, and facial recognition data is particularly sensitive. Furthermore, individuals who posted their images online, or whose images were posted by third party(ies), had no reasonable expectations that Clearview would collect, use and disclose their images for identification purposes. As such, express consent would generally be required. In Quebec, such use of biometric data requires express consent.

Clearview did not attempt to seek consent from the individuals whose information it collected. Clearview asserted that the information was "publicly available", and thus exempt from consent requirements. Information collected from public websites, such as social media or professional profiles, and then used for an unrelated purpose, does not fall under the "publicly available" exception of PIPEDA, PIPA AB or PIPA BC. Nor is this information "public by law", which would exempt it from Quebec's Private Sector Law, and no exception of this nature exists for other biometric data under LCCJTI. Therefore, we found that Clearview was not exempt from the requirement to obtain consent.

Furthermore, the Offices determined that Clearview collected, used and disclosed the personal information of individuals in Canada for inappropriate purposes, which cannot be rendered appropriate via consent. We found that the mass collection of images and creation of biometric facial recognition arrays by Clearview, for its stated purpose of providing a service to law enforcement personnel, and use by others via trial accounts, represents the mass identification and surveillance of individuals by a private entity in the course of commercial activity. We found Clearview's purposes to be inappropriate where they: (i) are unrelated to the purposes for which those images were originally posted; (ii) will often be to the detriment of the individual whose images are captured; and (iii) create the risk of significant harm to those individuals, the vast majority of whom have never been and will never be implicated in a crime. Furthermore, it collected images in an unreasonable manner, via indiscriminate scraping of publicly accessible websites.

We identified certain other concerns on which we did not ultimately opine, but which we felt appropriate to raise in our report. This includes the fact that there were credible challenges to, and questions regarding, the efficacy and accuracy of facial recognition technologies generally, and regarding the reliability of Clearview's testing results specifically.

We shared our preliminary findings and recommendations with Clearview, with a view to bringing it into compliance with federal and provincial private sector privacy law. We recommended that Clearview: (i) cease offering its facial recognition tool to clients in Canada; (ii) cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada; and (iii) delete images and biometric facial arrays collected from individuals in Canada in its possession.

Clearview expressly disagreed with our findings.

In disagreeing with our findings, Clearview alleged an absence of harms to individuals flowing from its activities. In our view, Clearview's position fails to acknowledge: (i) the myriad of instances where false, or misapplied matches could result in reputational damage, and (ii) more fundamentally, the affront to individuals' privacy rights and broad-based harm inflicted on all members of society, who find themselves under continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images.

In terms of remedies, noting that it had withdrawn from the Canadian market during our investigation, Clearview stated that it was "prepared to consider" remaining outside of the Canadian market for a further two years, while our Offices developed relevant guidance. Clearview suggested that it would be appropriate for our Offices to suspend our investigation and not issue this final report, and that during such a suspension, it "would be willing to take steps, on a best efforts and without prejudice basis, to try to limit the collection and distribution of the images that it is able to identify as Canadian" [emphasis added]. Clearview has not committed to following our recommendations. The Offices view it as inappropriate to suspend the investigation and not issue this Report. We therefore find the matter to be **well-founded** and restate the recommendations in our preliminary findings.

Additionally, the CAI determined that contrary to the requirements of the LCCJTI, Clearview had not advised the CAI that it had created a database of biometric characteristics, nor obtained the express consent from individuals that verifying or confirming their identity would be conducted using a facial recognition process.

Background

1. This report of investigation examines Clearview AI, Inc.'s (Clearview) compliance with Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* (Quebec's Private Sector Act), and *Act to Establish a Legal Framework for Information Technology* (LCCJTI), British Columbia's *Personal Information Protection Act* (PIPA BC), and Alberta's *Personal Information Protection Act* (PIPA AB) – referred to collectively as the Acts.

2. Clearview is a technology company headquartered in the United States that developed and delivered its facial recognition[4] software and combined database solution (App) to clients around the world. Clearview's App allows clients to upload a digital image of an individual's face and run a search against it. The App then applies its algorithm to the digital image and runs the result against Clearview's database to identify and display likely matches and associated source information.

[4] Facial Recognition generally refers to a category of biometric software that maps an individual's facial features mathematically and stores the data as a faceprint.

3. In January and February 2020, public reports[5] indicated that Clearview was populating its facial recognition database by collecting digital images from a variety of public websites, including but not limited to, Facebook, YouTube, Instagram, Twitter and Venmo, in apparent violation of those organizations' terms of service and without the consent of individuals. It was further indicated that these digital images were then indefinitely stored in Clearview's database to be sourced and served as results for facial recognition searches.

4. In February 2020, multiple reports[6] surfaced confirming that a number of Canadian law enforcement agencies and private organizations[7] had used Clearview's services in order to identify individuals.

5. Satisfied that reasonable grounds existed to investigate these matters, in February 2020, the Office of the Privacy Commissioner of Canada (OPC), the Commission d'accès à l'information du Québec (CAI), the Information and Privacy Commissioner for British Columbia (OIPC BC), and the Information and Privacy Commissioner of Alberta (OIPC AB), collectively referred to as the Offices, each initiated investigations pursuant to s.11(2) of PIPEDA, s.81 of Quebec's Private Sector Act, s.36(1)(a) of PIPA BC, and s.36(1)(a) of PIPA AB respectively. The Offices decided to conduct the investigation jointly in order to maximize their expertise and their resources, while avoiding duplication of their efforts and those of Clearview.

Issues

6. The issues in this investigation were:

   i. Whether Clearview was required under the Acts to get consent for its collection, use and disclosure of personal information and if so, whether it did; and

   ii. Whether Clearview collected, used and/or disclosed personal information for a purpose that a reasonable person would consider appropriate in the circumstances, for a purpose that was reasonable and to fulfill a legitimate need?[8]

7. The following Quebec-specific issue was also examined:

   i. Did Clearview previously disclose to the CAI the creation of a database of biometric characteristics or measurements?

---

[5] Hill, K. "The secretive company that might end privacy as we know it," *The New York Times*, January 18 2020; Fan, K., "Clearview AI responds to cease-and-desist letters by claiming first amendment right to publicly available data," *Harvard Journal of Law and Technology*, February 25 2020.

[6] "Toronto Police admit using secretive facial recognition technology Clearview AI," *CBC*, February 13 2020; Gillis, W., Allen, K., "Peel and Halton police reveal they too used controversial facial recognition tool," *The Star*, February 14 2020.

[7] Allen, K. et al, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known," *The Star*, February 27 2020.

[8] Throughout this report, the term "appropriate purpose" will be considered inclusive of "reasonable purpose" under PIPA AB and PIPA BC and "legitimate need" under Quebec's Private Sector Act.

8. During the course of the investigation, specifically after the letter of intention referred to in paragraph 11 below, Clearview also asserted that our Offices do not have jurisdiction over the Clearview activities in question. We address this issue in our analysis, prior to considering the issues identified above.

Methodology

9. In addition to conducting extensive open-source research, the investigative team (the team) analyzed representations provided by Clearview and records relating to its activities. The team also examined representations from a number of third parties identified as possible users of Clearview's service.

10. Between February and November 2020, Clearview provided multiple sets of written representations to our Offices. Furthermore, we gave Clearview multiple opportunities to meet with us to make inquiries and provide additional evidence. We conducted two such meetings in June 2020.

11. Upon completion of the evidence-gathering phase of the joint investigation, our Offices issued a letter of intention to Clearview on October 29 2020, which set out and explained the rationale for our preliminary findings, identified several orders and recommendations under consideration and invited Clearview to respond. We then met with Clearview on November 17 to clarify our views, provide an opportunity to ask any questions, and discuss potential remedies to resolve the matter. On November 20, Clearview provided a written response articulating its disagreement with our preliminary findings and orders and recommendations under consideration. In this letter, Clearview set out a variety of new arguments, and provided new information which our Offices considered and assessed before producing this report of findings.

Clearview's representations and our investigation

12. This section reflects initial representations provided by Clearview up to the point of the issuance of our letter of intention. Further representations provided by Clearview in its response to our letter of intention are included under our analysis of each issue.

Overview of Clearview's facial recognition implementation

13. In its submissions, Clearview explained that its facial recognition technology is based on five primary components: (i) image crawler, (ii) image store, (iii) metadata store, (iv) neural network and (v) vector database. The image crawler is an automated tool that searches public web pages and collects any images that it identifies as containing faces along with associated metadata such as the title, source link and description. This process is commonly referred to as "scraping." The images and metadata collected through this scraping process are indefinitely stored on Clearview's servers in the image and metadata stores respectively. The neural network underpins the algorithm that analyzes digital images of faces and turns them into numerical representations referred to as "vectors". Clearview's vectors consist of 512 data points that represent the various

unique lines that make up a face. Clearview then stores all of these vectors in their vector database, where they are associated with the images stored on Clearview's server. Every image in the database has a vector associated with it in order to allow identification and matching.

14. When an App user wishes to identify an individual, they are required to upload an image of their target into the App and run a search. The neural network then analyzes the image and produces a vector. This vector is then compared against all vectors stored in Clearview's database, with the App pulling any matching images from the vector database and providing them to the user, along with any associated metadata, as search results. Clearview stated that images uploaded by users are stored separately from images obtained from scraping, and do not show up in any search results.

15. Clearview advised that its search results are displayed in a list containing thumbnail images that appear to be a match for the individual, the name of the image, description and source link. The user must then click the associated source link to be re-directed to the web page where the image was originally collected, in order to obtain additional information. Clearview stated that it "[does] not possess or maintain any information about names, addresses, nationality, date of birth [or] location" associated with the images in its database.

Clearview's privacy practices regarding consent

16. Clearview originally stated that it does not seek consent from individuals whose information it collects. Rather, Clearview stated that in its view, the images it collected were publicly available and therefore it did not require the knowledge or consent of individuals to collect their information.

17. In support of this position, Clearview stated that it only collected images from publicly-viewable web pages, and did not collect any images protected by privacy settings, such as those associated with certain social media accounts, or from pages that enabled "robots.txt".[9] Clearview has confirmed that their image crawler is configured to respect whatever instructions are present in the robots.txt file.

Clearview's purposes

18. In its initial representations, Clearview advised our Offices that its App was intended to be for the sole and exclusive use of law enforcement. This was reflected in Clearview's terms of service, which state that "Users may use [the] Service for legitimate law enforcement and investigative purposes" and that "users may not use the Service for any reason other than law enforcement or investigative purposes." In response to our letter of intention, Clearview advised that previously, its terms of service also extended access to "security professionals".

[9] Robots.txt is a file that can be set up by the administrators of a webpage to instruct web crawlers regarding what pages or content they may or may not access. We note that abiding by the robots.txt file is optional, and can be disregarded by crawlers.

19. Clearview asserted that their technology provides "substantial, concrete benefits to public safety by dramatically increasing law enforcement's ability to identify and investigate suspects, victims and witnesses." Clearview pointed to numerous successes in cases ranging from "murder, armed robbery and child sexual exploitation to terrorism, major narcotics trafficking and multi-million dollar fraud."

20. When asked to speak to potential harms to Canadians that could arise from its technology, Clearview stated that any such harms were only hypothetical. Clearview stated that any "harm that a person would suffer from a Clearview search of their image is comparable to the harm that the person suffers when a Google search of his or her name is performed." Clearview further indicated that no single user could browse their full database as results were only provided for matches, thus mitigating any risk.

21. Clearview stated that even if its database were to be compromised and released, the images therein are all already accessible online, and thus not sensitive, and the vectors that it uses for biometric matching are hashed,[10] so they are useless outside of the Clearview App.

22. While Clearview originally allowed a variety of public and private organizations to create accounts, we note that in response to our investigation, Clearview stated that it had suspended access to all users in Canada, outside the RCMP, in March 2020. Following further engagement with our Offices during the investigation, Clearview voluntarily exited the Canadian market in July 2020.

Comparison with other organizations

23. Clearview asserted that its App is essentially an image search engine and asked our Offices why we were "treating them differently from other search engines".

24. This investigation focuses on Clearview's practices and not on those of the search engines cited by Clearview. Our Offices initiate and conduct investigations into organizations on the basis of each case's own particular set of facts. As such, we do not express an opinion on the obligations of any other organizations in this report.

Analysis

Clearview's jurisdictional challenge

25. At the latter stages of our investigation, subsequent to receiving the letter of intention from our Offices seeking a response to the preliminary findings in this matter, Clearview argued that none of our Offices have jurisdiction over its activities, asserting that "[n]one

[10] Hashing is a cryptographic technique, which consists of using a one-way function to transform data into a unique string. Hashing offers protection against reverse engineering (or other means aimed at recovering the original value) both by the organization collecting and holding the information and by third parties.

of Clearview's activities take place in Canada" and that it "is of the view in the circumstances that none of the statutes invoked apply and that no connecting factors create a real and substantial link to Canada." Clearview submitted that PIPEDA does not apply "because there is no real and substantial connection to Canada."

26. Specifically, Clearview argued that the circumstances in the matter at hand were such that no real and substantial connection with Canada existed:

    i. the content referred to in Clearview's platform was not "uniquely Canadian" and that it has content from "several other countries all over the world";

    ii. Clearview's services were "not directly and solely directed at Canadians" and that "not many Canadians would have used [its] services", asserting that "beyond the trial users, the only allegation is that one Canadian entity, the RCMP, would have used Clearview's services"; and

    iii. "there [appeared] to be no evidence that Clearview's services are mainly felt by Canadians".

27. Clearview further argued that it is not subject to any provincial privacy laws as in its view:

    i. it did not collect, use or disclose personal information "within the provinces of Alberta, Quebec or British Columbia, but rather in the United States";

    ii. there was "no evidence or allegation" that Clearview did business within said provinces; and

    iii. collection, use or disclosure had to take place entirely within each province to be applicable under the acts, and that there is "no evidence or allegation" that this took place.

OPC's jurisdiction

28. The OPC notes that PIPEDA applies to organizations outside of Canada where a "real and substantial connection" to Canada exists.[11] In our view, the circumstances in this matter clearly demonstrate that a real and substantial connection to Canada exists. In coming to this conclusion, we considered the relevant connecting factors that flow from the jurisprudence, including the factors set out in *A.T. v. Globe24h*: (1) the location of the target audience of the website, (2) the source of the content on the website, (3) the location of the website operator, and (4) the location of the host server.[12]

[11] *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 427 at paras 54-63.

[12] *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 FCR 310.

29. Regarding the location of Clearview's target audience:

    i. While Clearview claims that its activity in Canada was limited, this is at odds with the fact that it actively marketed its services to Canadian organizations through promotional material, testimonials from Canadian law enforcement professionals, and agency-specific presentations and trials. Furthermore, Clearview publicly declared Canada to be part of its core market in statements to the media[13] and its own promotional materials.[14]

    ii. The fact that only one agency became a paying customer is, in our view, immaterial. The colour and character of Clearview's activities were commercial in nature, with trials existing for the express purpose of enticing the purchase of accounts. Clearview's representations confirmed that 48 accounts (trial or otherwise) were created for law enforcement agencies and organizations across Canada, and thousands of searches were conducted through these accounts. In particular, we note that various provincial law enforcement agencies used trial accounts of the App for several months, with the number of searches conducted per trial account ranging from tens, to hundreds, or in one case, thousands**.** Furthermore, dismissing the RCMP as only "one Canadian entity" ignores the fact that the RCMP is Canada's national law enforcement agency, operating all over Canada with national, federal, provincial, and municipal policing mandates.

30. Regarding the source of Clearview's content:

    i. It is not a requirement that Clearview's content be exclusively derived from Canadian sources for there to be a real and substantial connection to Canada.

    ii. As set out in *Lawson v. Accusearch Inc*., it is not necessary to identify specific Canadian sources of content to determine we have jurisdiction.

    iii. Clearview's assertion that it collects images without regard to geography or source does not preclude our jurisdiction when a substantial amount of its content is sourced from Canada. The exact number of images derived from individuals in Canada is unknown due to the fact that Clearview does not retain the national source. However, the indiscriminate nature of Clearview's scraping renders it a relative certainty that it collected millions of images of individuals in Canada,[15] and used them to derive biometric image vectors for its database, including to market to Canadian law enforcement agencies.

---

[13] Mac, R. *et al*, "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA," *Buzzfeed News*, February 27, 2020.

[14] Archived Clearview AI Website.

[15] In 2017 Facebook released data showing that there were 23 million active Canadian accounts on Facebook and 8.5 million accounts on Instagram (an image-focused service). Canadians had shared 1.429 billion photos and 79 million videos on Instagram and shared an average of 2 million photos a day. Shankar, B. "Facebook has 23 million monthly users in Canada," *MobileSyrup*, June 21, 2017.

31. Finally, regarding the location of Clearview's website operations and host server:

    i. We note that Clearview's activities take place exclusively through a website or app. As referenced in paragraph 54 of *A.T. v. Globe24h.com*, a physical presence in Canada is not required to establish a real and substantial connection when considering websites under PIPEDA, as telecommunications occur "both here and there."

    ii. Clearview's operations necessitate the transmission and receipt of personal information between Canada and the USA, both when collecting information and disclosing it through its software.

    iii. As set out by the Supreme Court of Canada:[16] "Receipt may be no less "significant" a connecting factor than the point of origin (not to mention the physical location of the host server, which may be in a third country)."

Provincial jurisdiction

32. We further reject Clearview's assertion that it is not subject to PIPA AB, PIPA BC or Quebec's Private Sector Act (the Provincial Acts), respectively, and are of the view that Clearview's activities fall under the jurisdiction of both the OPC and the provinces.[17]

33. Provincial privacy legislation applies to any private sector organization that collects, uses and discloses information of individuals within that province. Clearview's practice of indiscriminate scraping has undoubtedly resulted in the collection of the personal information of individuals within Quebec, Alberta and British Columbia, whose residents collectively account for nearly half of the Canadian population. In addition, provincial and municipal law enforcement agencies located within the provinces and subject to provincial oversight were targeted and used trial accounts of Clearview's software, in the course of which they provided, and Clearview collected, personal information in the form of photographs of individuals.[18]

34. Clearview is a commercial enterprise that collected, used, and disclosed personal information of individuals within Quebec, Alberta and British Columbia with the intention of selling a product to law enforcement agencies within the provinces. The fact that a company is located outside of Quebec, Alberta and British Columbia, does not mean it

---

[16] *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.

[17] *Bell Mobilité*, CAI 1005977-S, decision by D. Poitras, February 5, 2020 [in French].

[18] Smith, A., "After officers tested Clearview AI, Calgary police improving tracking system for new technologies," *Calgary Herald*, March 11, 2020; Carney, B., "Despite Denials, RCMP Used Facial Recognition Program for 18 Years," *The Tyee*, Mars 10, 2020; "Une application utilisée par la police peut identifier les gens à partir d'une seule photo", *Radio-Canada*, January 20, 2020 [in French]; Péloquin, T., "Reconnaissance faciale: le SPVM refuse de dire s'il utilise un logiciel controversé", *La Presse*, February 18, 2020 [in French]; Bronskill, J., "RCMP facing proposed class action over use of Clearview AI's facial-recognition technology," *The Globe and Mail*, July 13, 2020; documents provided by Clearview.

can evade obligations under Quebec's Private Sector Act, PIPA AB and PIPA BC. Indeed, whenever a company collects the personal information of individuals located within a province, regardless of where the company is located, the Provincial Acts apply.[19]

35. Considering the above, the Offices do not accept Clearview's assertion that provincial legislation does not apply and are of the view that:

    i. the Provincial Acts apply, as previously stated;

    ii. the Provincial Acts do not prevent the achievement of PIPEDA's objective, nor do they result in operational conflict or conflict of intent;

    iii. each Provincial Act has been found to be substantially similar to PIPEDA.[20]

Issue 1: Did Clearview obtain requisite consent?

36. In our view, Clearview did not obtain consent required for its collection, use and disclosure of personal information through the App. In coming to this determination, we note that Clearview made no attempt whatsoever to obtain consent from individuals, given its erroneous interpretation of Canadian privacy law, which sets out when information is "publicly available" or "public under the law".

37. The Acts state that the consent of the individual is required for the collection, use or disclosure of personal information unless an exception applies.[21] The type of consent required will vary depending on the circumstances and the type of information involved.

38. The Guidelines for obtaining meaningful consent[22] (the Guidelines) jointly issued by the OPC, OIPC AB and OIPC BC provide that "organizations must generally obtain *express* consent" when: (i) the information being collected, used or disclosed is sensitive; (ii) the collection, use or disclosure is outside of the reasonable expectations of the individual; and/or (iii) the collection, use or disclosure creates a meaningful residual risk of significant harm.

---

[19] *Firquet c. Acti-Com*, 2018 QCCAI 245 (CanLII); *Serres Floraplus inc. c. Norséco inc.*, 2008 QCCS 1455 (CanLII); Douville, D., Privacy and Security, *Fasken Bulletin*, May 16, 2019; Geist, M., "Is there a there there ? Toward greater certainty for internet jurisdiction," *Berkeley Technology Law Journal, Vol. 16, #3, p. 1345 (2001)*.

[20] *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219, *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220, *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.

[21] *PIPEDA* sections 5(1), 6.1 and 7 as well as principle 4.3 of Schedule 1, *PIPA AB* section 7, *PIPA BC* sections 6-8, Quebec's *Private Sector Act* sections 6 and 12-14, and *LCCJTI* section 44.

[22] Guidelines for obtaining meaningful consent, *OPC*, 2018.

39. Beyond Clearview's collection of images, we also note that its creation of biometric information in the form of vectors constituted a distinct and additional collection and use of personal information, as previously found by the OPC, OIPC AB and OIPC BC in the matter of Cadillac Fairview.[23]

40. With respect to biometric characteristics and measurements, Quebec's LCCJTI specifically requires the express consent of the person concerned. Consent is described as express when it is explicit and unequivocal. To give express consent, a person must perform a positive action that clearly demonstrates his or her agreement.[24] To perform such an action, the person must be informed about what his or her consent entails.[25] The consent must be free, enlightened, given for specific purposes and limited in time.[26]

41. In our view, biometric information is sensitive in almost all circumstances. It is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual. That being said, within the category of biometric information, there are degrees of sensitivity. It is our view that facial biometric information is particularly sensitive. Possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the Internet, as demonstrated in the matter at hand, or via surreptitious surveillance.

42. For these reasons, it is our view that in the absence of an applicable exception, Clearview should have obtained express opt-in consent before it collected the images of any individual in Canada.

43. In its submissions, Clearview acknowledged that it did not seek consent from the individuals whose information it collected, used or disclosed. Clearview argued that the information it collected was "publicly available" and that there was thus no reasonable expectation of privacy.

44. Our Offices note that PIPEDA, PIPA BC and PIPA AB have exceptions to the requirement for consent where the personal information at issue is publicly available as set out in section 7(1)(d) of PIPEDA, sections 12(1)(e), 15(1)(e) and 18(1)(e) of PIPA BC, and sections 14(e), 17(e) and 20(j) of PIPA AB. The definition of "publicly available" is provided by each Act's regulations[27] and is distinct from a common understanding of "publicly accessible" information.

---

[23] Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia, *OPC, OIPC AB, OIPC BC*, paragraph 68.

[24] Biometrics: Principles and Legal Duties of Organizations – Practical Guide for Public Bodies and Enterprises, *CAI*, July 2020.

[25] *Act respecting the protection of personal information in the private sector,* section 8.

[26] *Act respecting the protection of personal information in the private sector*, section 14.

[27] Section 1 of PIPEDA's *Regulations Specifying Publicly Available Information*; Section 6 of *PIPA BC Regulations*, Prescribed source of public information and Section 7 of *PIPA AB Regulations*, Publicly available information.

45. Information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the "publicly available" exception of PIPEDA.[28] Similarly, the respective regulations of both PIPA AB and PIPA BC[29] prescribe sources of public information that include directories, registries, and publications. Social media websites and search engines are not listed as prescribed sources of publicly available information under either of these Acts. As such, collection from these sources would only be authorized with consent and only if the purposes are what a reasonable person would consider appropriate.[30]

46. Quebec's Private Sector Act and LCCJTI do not distinguish, and make no allowance for, "publicly available information." However, Quebec's Private Sector Act does not apply to information "which by law is public." There are no Quebec statutes under which personal information is deemed to be public solely based on the fact that it has been posted on social media or the Web. Moreover, the CAI has previously ruled that, even where personal information has been posted on a public website, it does not mean that the information may be used for other purposes without the consent of the person concerned.[31] The fact that images are published on a website does not necessarily mean that their author has consented to their use by a third party.

47. As such, our Offices do not recognize the personal information collected, used or disclosed by Clearview to be "publicly available" as envisioned by the Acts, or as information "which by law is public," and thus the exception does not apply.

48. As Clearview made no attempt to obtain consent, and no exception from the requirement to obtain consent is found to be applicable, we find that Clearview contravened sections 6.1 as well Principle 4.3 of Schedule 1 of PIPEDA, section 7 of PIPA AB, sections 6-8 of PIPA BC, sections 6 and 12-14 of Quebec's Private Sector Act and section 44 of the LCCJTI.

Clearview's response regarding consent

49. In its response, Clearview stated that:

> "With respect to the consent obligation under federal and provincial legislation, and assuming, without waiving the lack of jurisdiction invoked above that such laws apply, Clearview submits that the exception for publications which are publicly available applies. Information collected by Clearview is nothing more than information available to the public."

---

[28] Company's re-use of millions of Canadian Facebook user profiles violated privacy law, *OPC*, paras 112-113.
[29] Section 7 *of PIPA AB Regulations*; Section 6 of *PIPA BC Regulations*.
[30] Always, sometimes, or never? Personal information & tenant screening, *OIPC BC*, 2018.
[31] Confédération des syndicats nationaux, CAI 1009621-S et 1009629-S, decision by C. Chassigneux, November 12, 2019 [in French]. See also *Quebec's Private Sector Act*, section 13.

50. Clearview argued that its collection of information qualified under the exception set out in regulation for "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."[32] In regard to Quebec's legislation, which does not contain such exceptions, Clearview argued that the exception must necessarily be implied. It argued that otherwise, "the legislation is invalid because it breaches the Quebec and Canadian Charter guarantees of freedom of expression."

51. The respondent further argued that the regulatory definition of publicly available information "is not distinct from the common understanding of the words" and that while Parliament "did define some categories of items that may be included in what is said to be public, it did not restrict the definition with respect to publication," stating that:

> "In Clearview's submission, the definition [of a publication] could hardly be broader. As a result, personal information located on public blogs, public social media or any other public websites are included in the "publicly available" exception as they are included in the definition of a publication. Therefore, the collection of such information does not require consent."

52. In support of its position, Clearview cited the Federal Court of Appeal's decision in *Lukács v. Canada,*[33] stating that "this decision makes it clear that these terms are not narrow and include any publication that is "*available or accessible by the citizenry at large.*"

53. Clearview further submitted that the expectation of privacy for information in the public view "is or should be reduced" and that a broad interpretation of publicly available information should be preferred, stating:

> "Even if the regulation and its exceptions are ambiguous, and require an exercise in interpretation, they must be interpreted in accordance with the Canadian Charter. Restricting the free flow of publicly available information is contrary to the constitutional protection of freedom of expression. For this reason, exceptions to this principle must be narrowly construed and a broad interpretation of publicly available must be preferred so as not to unduly limit freedom of expression."

54. Finally, Clearview argued that:

> "In these circumstances, […] the positive effects of protecting personal information do not outweigh the negative effects on Clearview's freedom of expression. There is no pressing and substantial concern justifying an infringement on freedom of expression given the lack of a reasonable expectation of privacy in images that individuals themselves have already either placed or permitted to be placed in the public domain."

---

[32] Section 1(e) of PIPEDA's *Regulations Specifying Publicly Available Information*; Section 6 of *PIPA BC Regulations*, Prescribed source of public information and S*ection 7 of PIPA AB Regulations*, Publicly available information.
[33] *Lukács c. Canada (Transport, Infrastructure et Collectivités),* 2015 CAF 140 (CanLII), para. 69.

55. Based on these arguments, Clearview asserted that it did not contravene any of the Acts, as all of the information it collected and used was exempted as publicly available.

56. As we note in paragraph 36, Clearview did not make any attempt to seek consent from individuals. Instead Clearview relies entirely on its argument that the personal information it collected, used and disclosed was publicly available and thus exempted from consent requirements. In considering Clearview's submissions, our Offices have concluded that this view is incorrect, and that the exemption does not apply in the circumstances of this case.

57. As set out in PIPEDA and confirmed in *Turner v. Telus Communications Inc*.[34], information will only be deemed "publicly available" if both publicly available **and** specified by the regulations.

58. Clearview further argued that a "plain language" interpretation of the regulations was appropriate, and that it followed that a broad definition of the term "publication," should be applied when considering whether the exemption applies. Clearview further argued that such a broad interpretation would be in accordance with the Canadian Charter of Rights and Freedoms (the Charter), namely freedom of expression.

59. We do not accept this to be the case based on the facts, law or available jurisprudence as outlined below.

60. It is our view that *Lukács c. Canada* is not applicable to the matter at hand, as it concerns the application of the Privacy Act, which is distinct from PIPEDA. In particular, we note that unlike in the *Privacy Act*, the meaning of "publicly available information" and what qualifies as a "publication" is specifically defined in PIPEDA, PIPA AB[35] and PIPA BC[36] by regulation (the Regulations). The Regulations thus take precedence.

61. When interpreting the Regulations, we note that as privacy legislation is considered by the courts to be quasi-constitutional,[37] the rights accorded under them should be given a broad, purposive and liberal interpretation, and restrictions on those rights should be interpreted narrowly.[38]

---

[34] *Turner v. Telus Communications Inc.,* 2005 FC 1601 at paragraphs 50 & 54.

[35] *Section 7 PIPA AB Regulations*.

[36] *Section 6 PIPA BC Regulations*.

[37] For example in: *Nammo v. Transunion of Canada Inc.,* 2010 FC 1284 at paragraphs 74 and 75; Bertucci v. Royal Bank of Canada, 2016 FC 332 at para. 34; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 paragraphs 19 and 22; *Cash Converters Canada Inc. v. Oshawa (City)*, 2007 ONCA 502 (CanLII) at para 29 citing *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 (CanLII), [2002] 2 S.C.R. 773 and *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403.

[38] *Qué*bec (Commission des droits de la personne et des droits de la jeunesse) v. Montréal (City); Québec (Commission des droits de la personne et des droits de la jeunesse) v. Boisbriand (City), 2000 SCC 27 (CanLII),

62. Since the Regulations create an exemption to a core privacy protection – the requirement for collection, use and disclosure of personal information to be with consent - they should be interpreted narrowly. With this in mind, we do not accept Clearview's arguments in favour of a wider "plain language" interpretation.

63. For example, social media, from which Clearview obtained a significant proportion of the images in its database, is not specified as a "publication" in the language of the PIPEDA regulations. It is the OPC's view that social media web pages differ substantially from the sources identified in the PIPEDA regulations. As the OPC previously found in the matter of Profile Technology,[39] there are a number of key differences between online information sources such as social media, and the examples of "publications" included in 1(e):

    i. social media web pages contain dynamic content, with new information being added, changed or deleted in real-time; and

    ii. individuals exercise a level of direct control, a fundamental component of privacy protection, over their social media accounts, and over accessibility to associated content over time – for example, via privacy settings.

64. In addition, the OIPC BC also takes the position that social media websites are not prescribed sources of "publicly available" information, and any collection from these sources would only be authorized with consent and only if the purposes are what a reasonable person would consider appropriate.

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.[40]

66. Even if such web pages were to be considered "publications" in the meaning of the Regulations, which we do not accept, s.1 (e) of the PIPEDA Regulations and s. 7(e) of the PIPA AB Regulations specify that the exception only applies "where the individual has provided the information," or where "it is reasonable to assume that the individual that the information is about provided that information," respectively. As Clearview engages in mass collection of images through automated tools, it is inevitable that in many instances, the images would have instead been uploaded by a third party.

---

paras. 28-30.*; New Brunswick (Human Rights Commission) v. Potash Corporation of Saskatchewan Inc.*, [2008] 2 SCR 604, 2008 SCC 45 (CanLII), paragraphs 19, 65-67.

[39] See generally: Company's re-use for millions of Canadian Facebook user profiles violated privacy law, *OPC*, paragraphs 87-96.

[40] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, [2013] 3 S.C.R. 733 at para. 19, citing the purpose clause in Alberta's *Personal Information Protection Act*, which is similar to the purpose clause in PIPEDA and PIPA BC.

67. Clearview argued that Quebec's Private Sector Act implicitly includes an exclusion for "publicly available" personal information—because if it did not it would violate the freedom of expression. The CAI is of the view that argument cannot be accepted for the following reasons:

    i. The text of the Act clearly indicates that only information that is public "by law" is excluded, which does not include information that is otherwise available to the public in the absence of a law designating it as public.

    ii. As a quasi-constitutional law that takes precedence over other legislation in Quebec, and has the purpose of clarifying the exercise of rights conferred by the *Civil Code of Québec*, specifically the right to privacy, any exceptions must be interpreted restrictively.

    iii. Therefore, there exists no implied exclusion from Quebec's Private Sector Act for publicly available information not designated as public by law.

    iv. Because Clearview did not inform the AG as required by section 76 of the *Code of Civil Procedure*, the Commission cannot consider claims raised by Clearview suggesting that the *Act respecting the private sector* is inoperative. Indeed, such a review cannot take place if the Attorney General of Quebec has not been informed or been given an opportunity to make representations.

    v. Nor does it suffice to raise a freedom of expression violation. Clearview has neither explained nor demonstrated how its activities constitute the expression of a message relating to the pursuit of truth, participation in the community or individual self-fulfillment and human flourishing.[41]

Issue 2: Was Clearview collecting, using or disclosing personal information for an appropriate purpose?

68. In our view, for the reasons outlined below, Clearview's purpose for collecting, using or disclosing personal information was neither appropriate nor legitimate.

69. In accordance with the OPC's Guidance on inappropriate data practices: Interpretation and application of subsection 5(3),[42] the OPC considers the factors[43] set out by the courts in order to assist in determining whether a reasonable person would find that an organization's collection, use and disclosure of information is for an appropriate purpose

[41] Irwin Toy Ltd. v. Quebec (Attorney General), 1989 CanLII 87 (SCC), [1989] 1 SCR 927, pp. 976–977; Institut généalogique Drouin inc. c. Commission d'accès à l'information du Québec, 2017 QCCQ 7573 (CanLII) [in French].

[42] Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), *OPC*, 2018.

[43] 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.

in the circumstances. These factors are to be applied in a contextual manner, which suggests flexibility and variability in accordance with the circumstances.[44] In applying s.5(3), the courts have determined that the OPC is required to engage in a "balancing of interests" between the individual's right to privacy and the commercial needs of the organization concerned.[45] This balancing of interests must be "viewed through the eyes of a reasonable person."[46] Similar factors are also considered by OIPC BC in determining whether the purpose is reasonable.[47]

70. Section 2 of PIPA AB says that in determining whether a thing or matter is reasonable or unreasonable, the standard to be applied is "what a reasonable person would consider appropriate in the circumstances". Orders issued by the OIPC AB have also identified a number of questions for determining whether the collection of personal information in an instance was for a reasonable purpose,[48] including whether the collection of personal information was carried out in a reasonable manner.

71. Finally, in analyzing whether Clearview had a serious and legitimate reason to establish a file on another person under section 4 of Quebec's Private Sector Act, the CAI considers the lawfulness of the objective sought and its compliance with the law, justice and fairness.[49]

72. We find that the collection of images and creation of biometric facial recognition arrays by Clearview, for its stated purpose of providing a service to law enforcement personnel, and use by others via trial accounts, represents the mass identification and surveillance of individuals by a private entity in the course of commercial activity.

73. In our view, for the reasons outlined below, a reasonable person would not consider this purpose to be appropriate, reasonable, or legitimate in the circumstances, within the meaning of subsection 5(3) of the PIPEDA, sections 11, 14 and 17 of PIPA BC,[50] sections 11, 16 and 19 of PIPA AB and section 4 of Quebec's Private Sector Act.

74. As previously indicated, our Offices find the information at issue (facial biometrics generated from digital images) to be of a sensitive nature. Biometric information is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual. Facial biometric data is particularly sensitive given that it is a key to an individual's identity, supporting the ability to identify and surveil individuals.

---

[44] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, para 131.
[45] *Turner v. Telus Communications Inc.*, 2005 FC 1601, aff'd 2007 FCA 21.
[46] *Ibid.* [*Turner v. Telus Communications Inc.*, 2005 FC 1601, aff'd 2007 FCA 21].
[47] See, for example: OIPC BC Order P12-01 (2012 BCIPC No. 25); Order P13-02 (2013 BCIPC No. 24) and Order 20-04 (2020 BCIPCD No. 24).
[48] Order P2006-011 - The OIPC AB set out a number of questions for determining whether the collection of personal information was for a reasonable purpose, as follows: 1) Does a legitimate issue exist to be addressed through the collection of personal information? 2) Is the collection of personal information likely to be effective in addressing the legitimate issue? 3) Is the collection of personal information carried out in a reasonable manner?
[49] *Institut généalogique Drouin Inc.*, CAI 091570, decision by D. Poitras February 6, 2015 [in French].
[50] *Cruz Ventures Ltd. (Wild Coyote Club) (Re)*, 2009 CanLII 38705 (BC IPC) paras 135-136.

75. We further note that the additional contextual information provided via source links (that is, social media and websites) can include significant personal information of varying levels of sensitivity. Further, Clearview's collection of information includes the mass indiscriminate collection of the personal information of minors, which would be considered particularly sensitive.

76. It is our view that Clearview does not, in the circumstances, have an appropriate purpose, for:

    i. the mass and indiscriminate scraping of images from millions of individuals across Canada, including children, amongst over 3 billion images scraped world-wide;

    ii. the development of biometric facial recognition arrays based on these images, and the retention of this information even after the source image or link has been removed from the Internet; or

    iii. the subsequent use and disclosure of that information for its own commercial purposes;

    where such purposes:

    iv. are unrelated to the purposes for which the images were originally posted (for example, social media or professional networking);

    v. are often to the detriment of the individual (for example, investigation, potential prosecution, embarrassment, etc.); and

    vi. create the risk of significant harm to individuals whose images are captured by Clearview (including harms associated with misidentification or exposure to potential data breaches), where the vast majority of those individuals have never been and will never be implicated in a crime, or identified to assist in the resolution of a serious crime.

77. Furthermore, Clearview's collection of sensitive biometric personal information, as described above, was not, in our view, carried out in a legal manner. Clearview collects the information to populate its facial recognition database without obtaining express consent of the individuals in question, as required by the Acts, or any form of knowledge or consent for that matter.

78. Clearview did not collect the information directly from the individuals in question. Nor did it have any relationship with the third parties whose websites it scraped, who could have, hypothetically, obtained consent for Clearview's purposes. In fact, several of these third parties have made credible allegations that Clearview was not authorized to collect the information from their websites. As such, Clearview achieved its purposes via collection that inherently contravened Canadian privacy laws. Therefore, those purposes cannot in our view be considered appropriate.

79. Consequently, we find that Clearview contravened: subsection 5(3) of the PIPEDA, section 4 of Quebec's Private Sector Act, sections 11, 14 and 17 of PIPA BC and sections 11, 16 and 19 of PIPA AB.

Clearview's Response Regarding Appropriate Purposes

80. Clearview disagreed with our preliminary characterization of its purposes and stated that its collection of information was to "enable law enforcement agencies to obtain information quickly and accurately in the course of an ongoing investigation" and that a reasonable person would consider this purpose to be "appropriate, reasonable and legitimate in the circumstances." Clearview re-iterated its view that this information was publicly available and thus not sensitive.

81. Clearview asserted that:

> "the difference between the purposes for which the images were originally posted and the ones for which Clearview used, collected, or disclosed them is irrelevant. If the purposes underlying Clearview's actions are appropriate and legitimate, it is reasonable to believe that Clearview has complied with this section of the law even if such images are not used, collected or disclosed for the same reason they were posted originally."

82. Clearview also asserted that any detriment to individuals resulting from the use of its services could not be imputed to Clearview, stating that:

> "Prosecution by law enforcement agencies using Clearview's services is in no way a direct and unique consequence of the services offered. Clearview cannot be held responsible for offering services to an entity that subsequently makes an error in its assessment of the person being investigated. Many factors will be taken into account by law enforcement agencies when doing their work. Clearview provides potential matches – just as witnesses provide potential identification in a line-up or eye-witness testimony. Law enforcement officials must ultimately determine the suitable use to be made of such information in the course of their investigations."

83. Clearview argued that a characterization of its purposes as detrimental to individuals was incorrect, stating:

> "Clearview's objectives are not to the detriment of individuals, but rather to the benefit of the community and the public interest by assisting law enforcement agencies responsible for public safety in their inquiries. Limiting such a service would arguably be at the expense of the public interest. Clearview facilitates research by providing a platform that contains all the information needed, information that is already available but dispersed on several third-party websites."

84. Clearview further argued that the only potential harm to most individuals would be that a link to a photo might be sent to a law enforcement agency, which in their view could not be described as significant. It opined that such potential harm was not disproportionate to the "benefits and objectives to which [Clearview] contributes."

85. Clearview concluded by referencing the purpose clause of PIPEDA, stating that:

> "when determining whether there are appropriate purposes involved, one must evaluate the balance between the privacy right of an individual and the need of organizations to collect, use or disclose personal information."

and that:

> "Given the significant potential benefit of Clearview's services to law enforcement and national security on the one hand, and the fact that significant harm is unlikely to occur on the other, especially considering that the information held is already publicly available and is distributed to law enforcement agencies for legitimate investigative purposes only, Clearview's purposes are entirely appropriate."

86. We are not convinced by Clearview's arguments, which cite the same jurisprudence that we have relied on. We remain of the view, based on our analysis outlined above in paragraphs 73 to 78, that Clearview is collecting sensitive biometric personal information, for purposes that a reasonable person would not consider appropriate in the circumstances.

87. Whereas law enforcement agencies rely on the broad collection authority for their operations found in public-sector privacy legislation, these actions are circumscribed by the Charter and Clearview enjoys no such collection authority as a private organization.

88. 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.[51]

89. Finally, we note that Clearview emphasizes the absence of harms to individuals flowing from its activities. In taking this position, Clearview fails to acknowledge: (i) the myriad of instances where false, or misapplied matches could result in reputational damage to individuals, and (ii) more fundamentally, the affront to individuals' privacy rights and broad-based harm inflicted on all members of society, who find themselves under continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images.

Additional concerns in relation to appropriate purposes

90. We note a number of additional issues. We will not specifically opine on them, but we continue to have significant concerns about them in the context of Clearview's facial recognition practices.

[51] *Cash Converters Canada Inc. v. Oshawa (City),* 2007 ONCA 502 (CanLII) at para 38.

Accuracy

91. While our Offices did not complete a technical assessment of the accuracy of Clearview's facial recognition technology, we recognize a number of concerns related to facial recognition technology, generally.

92. Our Offices accept that facial recognition technologies may be used to render many services to society and individuals, and have a number of legitimate uses in business and government. For example we recognize that facial recognition can assist businesses with identity authentication, or law enforcement agencies in the investigation of serious and complex crimes. However, while facial recognition technology, and Clearview's technology in particular, may be effective in certain circumstances, we note that there are significant concerns regarding the efficacy and accuracy of facial recognition technologies, in particular with respect to certain demographics.

93. Despite advances in the sophistication of facial recognition technology through the increase of computational capacity, the improvement of underlying algorithms and the availability of huge volumes of data, such technologies are not perfect and can result in misidentification. This can be the result of a variety of factors, including the quality of photos/videos and the performance of algorithms used to compare facial characteristics. In particular, our Offices take note of claims of accuracy concerns stemming from a variety of studies and investigations of facial recognition algorithms found in a number of technology solutions.

94. Accuracy issues in facial recognition technology can take two general forms: (i) failure to identify an individual whose face is recorded in the reference database, referred to as a "false-negative"; or (ii) matching faces that actually belong to two different individuals, referred to as a "false positive." While the former is an issue primarily for the users of facial recognition technology, the latter presents compelling risks of harm to individuals, particularly when facial recognition is used in the context of law enforcement.[52]

95. In particular, we refer to reports that facial recognition technology has been found to have significantly higher incidences of false positives or misidentifications when assessing the faces of people of colour, and especially women of colour, which could result in discriminatory treatment for those individuals.[53] For example, research conducted by NIST (National Institute of Standards and Technology) found that the rate of false positives for Asian and Black individuals was often greater than that for Caucasians, by

[52] Angwin, J. *et al*.. "Machine Bias," *ProPublica*, May 23, 2016.

[53] See "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," *National Institute of Standards and Technology* (NIST), December 2019; "Black and Asian faces misidentified more often by facial recognition software," *CBC News*, December 2019, and "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," *Washington Post*, December 2019.

a factor of 10 to 100 times.[54] Harms resulting from such misidentification can range from individuals being excluded from opportunities, to individuals being investigated and detained based on incorrect information. Such harms would generally be classified as significant.[55]

96. We note that Clearview commissioned an independent panel to complete an accuracy test of their technology, which it claimed was based on the methodology of a previous test conducted by the American Civil Liberties Union (ACLU). A copy of the results from this test was provided in Clearview's representations, and reported a 100% accuracy rate for Clearview's technology. During our investigation we found that significant concerns, regarding the testing methodology and conclusions, had been raised by a variety of researchers, including the ACLU's own team, who characterized the study as "misleading," and lodged a complaint with Clearview.[56]

97. In its submissions, Clearview argued that the ACLU and other critics had failed to demonstrate how the results of the test were misleading. It reiterated that in testing, Clearview's App correctly matched all the images it searched for, with no inaccuracies. While our Office will not opine on the merits of such complaints, we do note the persistent theme of concerns raised in relation to the opacity of Clearview's technology, which is proprietary and inaccessible to the majority of researchers, make it difficult to make determinations on accuracy.

Collection in contravention of contractual terms

98. We note that Clearview has received cease-and-desist letters from Google, Facebook, Twitter, YouTube and LinkedIn regarding their practice of collecting information in violation of terms of service.[57]

99. Clearview represented that it has responded to these cease-and-desist requests by asserting a First Amendment right to scrape "public" information under the U.S. Constitution. Clearview also asserted that contractual terms have no bearing on our investigation or the appropriateness of its purposes.

100. While we do not opine on whether or not one or more contractual violations occurred, to the extent that Clearview scraped personal information in contravention of platforms' contractual terms, it would in our view, be relevant as a further factor in considering the inappropriateness of Clearview's purposes, in the circumstances.

---

[54] "Face Recognition Vendor Test, Part 3: Demographic Effects," *National Institute of Standards and Technology* (NIST), December 2019.

[55] Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), *OPC*, 2018.

[56] Haskins, C. *et al.*, "The ACLU Slammed A Facial Recognition Company That Scrapes Photos From Instagram And Facebook," *Buzzfeed News*, February 2020.

[57] Wood, C., "Facebook has sent a cease-and-desist letter to facial recognition startup Clearview AI for scraping billions of photos," *Business Insider*, February 6, 2020.

Risk of harm arising from breach

101. The large amount of sensitive biometric information held by Clearview would in our view, make it a high value target for malicious actors. Clearview argued that "risk of harm from breach is not an appropriate consideration when assessing the purposes of Clearview's actions, as this would go well beyond the scope of the law, which is to establish rules that recognize the right of privacy of individuals," claiming that this risk is present in "almost all areas of society." It further argued that even if such risks were taken into account, there was no risk of significant harm or likelihood of the information being stolen. While we will not opine on Clearview's safeguards, which are outside the scope of this investigation, we do note that Clearview publicly announced that it was breached on two occasions within the past year. Once in February 2020 when its client list was leaked,[58] and again in April 2020 when its source code and pilot project video were obtained and partially leaked.[59] In our view, Clearview's collection and subsequent use of billions of images and facial arrays which are linked to source data, represents a significant risk to tens of millions of individuals in Canada should it be compromised.

Issue 3: Did Clearview satisfy its biometric obligations in Quebec?

102. When a company builds a biometrics system in Quebec, it must comply with the rules set out in Quebec's Private Sector Act and the LCCJTI. Indeed, it must in particular:

    i. obtain the express consent of the person concerned, in line with s.44 of the LCCJTI; and

    ii. disclose the creation or existence of the biometrics system to the CAI in line with s.45 of the LCCJTI.

103. It is apparent from the investigation that Clearview failed to obtain the express consent of the persons concerned, as Clearview has acknowledged that no attempt to seek consent was made. Furthermore, the company failed to disclose the existence of its biometrics system to the CAI.

Clearview's response regarding Quebec's biometric law

104. Clearview argues that it did not build a biometric system in Quebec, since its activities take place in the United States. Noting that a provincial statute cannot apply extraterritorially in the absence of the express or implied will of the legislature, Clearview concludes that the LCCJTI cannot apply to it, because that would give the law extraterritorial scope that no provision could confer on it, whether explicitly or implicitly.

105. The CAI does not share Clearview's opinion with respect to the LCCJTI. Indeed, since Clearview does not deny having built a biometric system, the CAI is of the opinion that, even if the biometric system is located outside of Quebec, Clearview has nevertheless

[58] "Clearview AI: Face-collecting company database hacked," *BBC*, February 27, 2020.

[59] Whittaker, Z., "Security lapse revealed Clearview AI source code," *TechCrunch*, April 16, 2020.

collected images in the course of operating a business in Quebec and must therefore obtain the express consent of these individuals before verifying or confirming their identity.

106. The essence of the LCCJTI provisions at issue are respect for the privacy of the individuals concerned and the protection of their personal information. The intention that this mandatory obligation be applied to *all* persons is made very clear in the French version by the use of the word “nul”. The extraterritorial effects are incidental.

107. Clearview, by offering its services within the territorial boundaries of the province and collecting and using the personal information of Quebecers, is operating a business in Quebec. Accordingly, Clearview is subject to the applicable legislation in the jurisdiction in which it is carrying out its activities, namely, the province of Quebec.[60] Clearview’s physical location and the site of its principal activities are therefore incidental and do not shelter it from the application of the LCCJTI.

108. Therefore, Clearview must obtain the express consent of individuals before verifying or confirming their identity (s.44 of the LCCJTI), as noted in paragraph 40. The sensitivity of the information collected, used or disclosed and the impact that the use of this information may have on the privacy of the individuals concerned requires that they be informed and express their consent. A biometric system cannot be used without the knowledge of the individuals involved.[61]

109. Clearview was also required to disclose its database of biometric characteristics and measurements to the Commission, in accordance with section 45 of the LCCJTI.

110. Consequently, the CAI finds that Clearview contravened sections 44 and 45 of the LCCJTI.

Recommendations

111. In our letter of intention, we shared with Clearview that we could order or recommend to:

    i. cease offering the facial recognition services that have been the subject of this investigation to clients in Canada;

    ii. cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada; and

    iii. delete images and biometric facial arrays collected from individuals in Canada in its possession.

[60] *Attorney General (Que) v. Kellogg’s Co. of Canada et al.*, [1978] 2 S.C.R. 211 (CanLII).
[61] *Les 3 Piliers Inc.*, CAI 1018507-S, decision by C. Chassigneux, February 14, 2020 [in French].

112. With respect to the first recommendation, we asked Clearview to confirm that it would not resume its offer to provide the facial recognition services in Canada in the future. We also sought Clearview's commitments explaining how and when it would implement the second and third recommendations.

Clearview's response to our conclusions

113. As detailed in this report, Clearview expressly disagreed with our conclusions.

114. Despite this, noting that following engagement with our Offices, it had voluntarily withdrawn from the Canadian market earlier in the investigation, Clearview indicated that it was "prepared to consider maintaining this status for a further two years, in order to allow the various Commissioners to provide detailed and meaningful guidelines as to how Canadian law proposes to deal with artificial intelligence."

115. Clearview suggested that as it was not "currently active" in Canada, our Offices should suspend our investigation and refrain from issuing a report or making a final determination on this matter.

116. Clearview indicated that "during such a suspension, [it] would be willing to take steps, on a best efforts and without prejudice basis, to try to limit the collection and distribution of the images that it is able to identify as Canadian..."

117. As of the time of writing this report, Clearview had not committed to following our recommendations or orders under consideration, and the Offices deemed it appropriate to issue this report.

Conclusions

118. To conclude, we find that Clearview engaged in the collection, use and disclosure of personal information through the development and provision of its facial recognition application, without the requisite consent. Consequently, we find that Clearview contravened: principle 4.3 of Schedule 1, as well as section 6.1 of PIPEDA; section 7(1) of PIPA AB; sections 6-8 of PIPA BC; and sections 6 and 12-14 of Quebec's Private Sector Act.

119. We also find that Clearview's collection, use and disclosure of personal information through the provision of its facial recognition application was for a purpose that a reasonable person would find to be inappropriate. Consequently, we find that Clearview contravened: subsection 5(3) of PIPEDA; sections 11,16 and 19 of PIPA AB; sections 11, 14 and 17 of PIPA BC; and section 4 of Quebec's Private Sector Act.

120. Additionally, the CAI finds that Clearview does not comply with sections 44 and 45 of the LCCJTI, by using biometric information for identification purposes without the express consent of the individuals concerned and by not disclosing the database of biometric characteristics and measurements to the Commission.

121. For all the reasons above, and despite Clearview's position to the contrary, we find the matter to be **well-founded** and we recommend that Clearview:

    i. cease offering the facial recognition services that have been the subject of this investigation to clients in Canada;

    ii. cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada; and

    iii. delete images and biometric facial arrays collected from individuals in Canada in its possession.

122. We note Clearview's request that our Offices suspend our investigations, and its offer to take steps to limit the collection and distribution of the images of individuals in Canada. However, we do not agree that a suspension of our investigations would be appropriate. To the contrary, we find it is important to conclude our joint investigation, and in this particular case, to publish our findings and recommendations or orders in the public interest. Among other considerations, this will ensure that other organizations have the benefit of our conclusions as they contemplate initiatives that may share certain similarities with Clearview's practices.

123. Should Clearview maintain its refusal to accept the findings and recommendations of four independent Canadian privacy enforcement authorities, we will pursue other actions available to us under our respective Acts to bring Clearview into compliance with federal and provincial privacy laws applicable to the private sector.

.