# Comments on the Clearview AI joint Report of Findings

**February 11, 2021**

On February 3, 2021, 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 (AB OIPC, and together with the BC OIPC, the CAI and the OPC, the Regulators), published a joint Report of Findings (the Report) following an investigation into 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 private sector privacy laws (Privacy Laws).

In the wide-ranging Report, the Regulators characterize Clearview's activities as mass surveillance and as an affront to the privacy rights of individuals,[1] and cover such issues as the scope of the consent exception for publicly available information, whether Clearview's collection was for an appropriate purpose, and obligations relating to biometrics.

## Background

Clearview, a technology company based in the United States, created a facial recognition software system incorporating a database that links images obtained from a variety of online sources with (i) facial recognition data derived from those images and (ii) hyperlinks to the online source. The Clearview system allows clients to upload a digital image of an individual's face and run a search against it. The Clearview system then applies its facial recognition algorithm to the digital image, and runs the result against Clearview's database to identify and display likely matches and associated source information.[2]

In January and February 2020, news media reported that Clearview was populating its facial recognition database with digital images collected from a variety of public websites (predominantly social media), [3] and that a number of Canadian law enforcement agencies and private organizations had used Clearview's services in order to identify individuals.[4]

The Privacy Regulators opened a joint investigation into Clearview in February of 2020.

# Decision

The core aspects of the finding are unsurprising and align with existing jurisprudence and Regulator guidance.

The Regulators affirmed that both federal and provincial Privacy Laws apply to Clearview's activities,[5] and that information posted on public social media profiles does not qualify for the "publicly available" or "which by law is public" consent exceptions provided for in Canadian private sector privacy laws.[6] Early on in its discussion of the definition of publicly available information, the Report refers to a previous finding from the Office of the Privacy Commissioner of Canada, which concluded that information available on social media sites under the Personal Information Protection and Electronic Documents Act (PIPEDA).[7] The Report concludes that Clearview should have obtained consent.

Consistent with earlier findings,[8] the Report also concluded that facial biometrics are particularly sensitive personal information and that therefore Clearview should have obtained express, opt-in consent before it collected the images of any individual in Canada.[9]

Furthermore, the Report found that Clearview's purpose in creating its system is not a purpose that a reasonable person would consider appropriate, reasonable, or legitimate in the circumstances.[10] As such, even if Clearview had obtained consent (whether express or not), that consent would have been invalid.

The Report also sets out some general remarks in relation to appropriate purposes, including the known potential for systems similar to Clearview's to generate false positives,[11] the possibility that Clearview collected the personal information in breach of the terms of service for the various social media platforms,[12] and the risk of harm engendered by the creation of a massive centralized database of sensitive facial biometric data.[13]

Finally, the Report found that in Québec, Clearview's system falls within the scope of legislation requiring express consent for the collection of biometric information. Moreover, as a creator of a database of biometric characteristics or measurements operating in Quebec, Clearview ought to have reported the existence of that database to the CAI.[14]

# Commentary

### *Consent*

As mentioned, the Regulators affirmed that information posted on public social media profiles does not qualify for the "publicly available" or "which by law is public" consent exceptions provided for in Privacy Laws. As such, Clearview should have obtained consent.

Since Clearview had stated from the outset that it relied on such exceptions and did not seek consent, the Report could have ended its analysis at that point as dispositive of the

issue. Despite this, a considerable amount of space in the Report is given over to dissecting whether Clearview's purposes are appropriate.

It is likely that the Regulators were concerned to ensure that this decision would be future-proofed in relation to Bill C-11, which sets out new privacy legislation that would replace PIPEDA, as well as legislative changes that may eventually come to pass at the provincial level.

For example, the Bill duplicates PIPEDA's language for consent exceptions for publicly available information,[15] leaving the specifics to regulation. Concerns have been raised[16] about the pressure to expand the definition of publicly available information to include situations where individuals decide to post personal information on a public website.[17] If Bill C-11 passes into law, a new regulation would be drafted and, if the definition were expanded, the analysis provided in the Report might be weakened or eviscerated.

Moreover, even if the new definition of publicly available information provided for in a new regulation excluded social media and other public websites, another provision of Bill C-11 could be construed as permitting activities that Clearview engages in, such as scraping personal information from such sites. Section 18(2)(e) of Bill C-11 permits the collection and use of personal information without an individual's knowledge or consent in respect of a business activity "in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual".[18]

Given, however, that Bill C-11 also replicates PIPEDA's "appropriate purposes" provision, this analysis could still be used even where a consent exception applied.[19] As such, it seems likely that the Regulators thought it prudent to address the appropriateness of purpose in case Bill C-11 and potential reforms of the provincial privacy laws materially alter the Report's analysis relative to consent and exceptions thereto.

Organizations should therefore bear in mind that Canadian privacy regulators will likely approach future investigations and analysis with an eye to ensuring that their findings remain durable under C-11.

### *Appropriate purposes*

The section of the Report that discusses appropriate purposes concludes that "continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images" is an "affront to individuals' privacy rights".[20]

While that may be something of an overstatement, there is no question that the system created by Clearview *facilitates* surveillance, and can improve the surveillance capabilities of its clients. Depending on the other resources available to those client organizations, such use could rise to the level of mass surveillance in some cases.

In coming to the conclusion that Clearview's activities represented mass surveillance, the Report characterized the activities of Clearview as follows: the mass scraping of images of individuals, including children; the development of facial recognition arrays based on those images; and the collection of source links, all for commercial purposes unrelated to the original purpose for which the images were posted, and which may

have detrimental effects on or create a risk of significant harm to those individuals.[21] Taken altogether, the Regulators found that this is not a purpose that a reasonable person would consider appropriate, reasonable, or legitimate in the circumstances.[22]

This analysis, however, presents a problem. Apart from the development of facial recognition arrays, search engines routinely undertake all of the activities listed, for commercial purposes that arguably introduce the potential for detrimental effects.

In this context, it is important to note that the Report also makes a comment in response to Clearview's concern that its activities were being treated differently from those of other image search engines,[23] stating that the investigation was focused on Clearview's practices and that the Report does not "express an opinion on the obligations of any other organizations".[24] The Regulators were clearly aware that characterizing Clearview's platform as a search engine could require the Report to enter into analysis of the fraught territory of search engine activities such as crawling, scraping and indexing.[25]

In consequence, although the Report ties the inappropriate purpose conclusion to the abovementioned multiplicity of factors, when one considers the Report's repeated emphasis on the biometric information generated by Clearview and the comment that the Report's findings express no opinion in respect of other organizations that Clearview regards as similarly situated, it is reasonable to conclude that the core concern lies with the development of facial recognition arrays based on the images collected. This aligns with earlier recent findings that demonstrate an elevated concern among the Regulators in relation to facial biometric technology, even when its use is not directed at identification.[26]

If this conclusion is correct, reverse image search engines that do not use facial biometrics in order to process search requests and provide results, and other systems or services that engage in mass collection of information would not necessarily be caught up by the appropriate purposes analysis provided in the Report.

Of course, engaging in the other activities mentioned may create other privacy law challenges to navigate. Even if those other challenges are successfully met, however, organizations should be alert to the possibility that adding facial biometrics to the mix could risk "poisoning" the purpose as a whole.

### *Biometrics*

The Report's finding that Clearview ought to have obtained express consent for its collection of biometric information in order to conform with section 44 of Quebec's *Act to establish a legal framework for information technology* signals that this provision is to be read broadly. This comes as no surprise.

It is possible to make artful arguments to the effect that systems such as Clearview's do not fit the canonical form of identification systems, since no attempt is made by Clearview itself to ensure that its database contains accurate identifying information (unlike, for example, a fingerprint database used by law enforcement). For example, source links may or may not provide identifying information: the individual may have created their profile under a nickname, or an image may have been scraped from a profile belonging to a third party.

However, it is difficult to deny that Clearview's general approach fits the description of identification systems given by the Quebec CAI in its guidance: systems designed to find "a specific identity from a set of identities stored in a database. The biometric characteristics and measurements of a person whose identity is unknown are compared with those in the database to answer the question: "Who is this person?"[27] Clients of Clearview evidently subscribe to its service in order to answer this question.

In consequence, the fact that Clearview's system may be unreliable and deliberately takes a minimal approach with respect to the quality of its sources is not enough to exclude it from being characterized as an identification system.

# Key takeaways

- Organizations should take note that Canadian privacy regulators will likely approach investigations and analysis with an eye to ensuring that their findings remain durable under Bill C-11 and anticipated reforms to provincial Privacy Laws.

- With respect to any given project or initiative involving the collection and use of personal information, the introduction of facial biometric technology raises the risk of a negative finding from Canadian privacy regulators on the grounds that the purpose is inappropriate.

- Among systems that permit or facilitate the identification of individuals, even those that are unreliable and deliberately take a minimal approach with respect to the quality of their sources may still be characterized as identification systems.

# Conclusion

As mentioned, the key findings of the Report are not surprising, and federal and provincial governments considering legal reforms to Canada's private sector privacy laws should certainly take the potential for activities such as Clearview AI's into account. Given the increased latitude that some of those reforms may provide in order to support beneficial innovation, and the likelihood that organizations will avail themselves of those flexibilities, in future we might expect to see more findings that rely on the appropriate purposes analysis where the Regulators wish to curtail certain activities.

The joint Report, reflecting a trend towards the issuance of such reports, also demonstrates a desire among the Regulators to show that they are materially aligned in outlook on various key issues. This is an encouraging development, as it creates an avenue for providing harmonized guidance of particular benefit to organizations with national operations. To the extent that provinces other than Alberta, British Columbia or Quebec decide to enact their own private sector legislation in future, such joint reports would also become crucial for navigating the Canadian privacy law landscape.

[1] Report para 72; See also OPC News Release, "Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say" February 3.

[2] Report, para 2.

[3] 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.

[4] "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; 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.

[5] Report, para 35.

[6] Report, paras 43-48.

[7] OPC, PIPEDA Report of Findings #2018-002, June 2018.

[8] 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.

[9] Report, para 42.

[10] Report, para 72.

[11] Report, paras 94 and 95, referencing "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.

[12] Report, para 100.

[13] Report, para 101.

[14] Report, para 105.

[15] Bill C-11, s. 51.

[16] See e.g. Teresa Scassa, "How Might Bill C-11 Affect the Outcome of a Clearview AI-type Complaint?", Feb 4 2021.

[17] See *Report of the Standing Committee on Access to Information, Privacy and Ethics*, February 2018, 42nd Parliament, First Session, p. 26-28.

[18] Bill C-11, s. 18(2)(e).

[19] Bill C-11, s. 12.

[20] Report, para 89.

[21] Report, para 76.

[22] Report, para 73.

[23] Report, para 23.

[24] Report, para 24.

[25] It is interesting to note that one of the key cases in which indexing forms part of the analysis, *A.T. v. Globe24h.com*, was cited solely in support of establishing whether there is a real and substantial connection to Canada in Clearview's case.

[26] See 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*.

[27] See CAI, *Biometrics: Principles and Legal Duties of Organizations*, July 2020.

By

Max Jarvie

Expertise

Cybersecurity, Privacy & Data Protection

---

**Montréal**

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

T 514.954.2555
F 514.879.9015

**Toronto**

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

T 416.367.6000
F 416.367.6749