# GPA Global Privacy and Data Protection Awards 2021

## Entry Form

To submit an entry to the GPA Global Privacy and Data Protection Awards please complete and email this form to secretariat@globalprivacyassembly.org **no later than 14 June 2021.**

Note: GPA member authorities can submit as many entries as they wish, but a separate form should be used for each different entry, submitted by the deadline above.

Languages: The GPA documentation Rule 6.2[1] applies.

## 1. CONTACT DETAILS FOR THIS ENTRY

| | |
|---|---|
| Privacy/Data Protection Authority: | **Office of the Privacy Commissioner of Canada (on behalf of the privacy authorities listed below)** |

## 2. ELIGIBILITY

By submitting this entry, I confirm that (*please tick all boxes to confirm)*:

☒ The Authority is a member of the Global Privacy Assembly

☒ The initiative described in this entry was undertaken since January 2020.

☒ I am aware that the information in the entry (other than the contact details in 1(a) above) will be publicised by the GPA Secretariat.

## 3. CATEGORIES

Please indicate which category you wish to enter.

*Please tick **one;** please use a separate form for each category you wish to enter:*

☐ Education and Public Awareness

☐ Accountability

☒ Dispute Resolution and Enforcement

☐ Innovation

☐ People's Choice

## 4. DESCRIPTION OF THE INITIATIVE

**a. Please provide a brief summary of the initiative** *(no more than 75 words)*

This past year, the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta, the Office of the Information and

[1] GPA Rules and Procedures, Rule 6.2 'Assembly documents':
Without prejudice to section 4.2, Assembly documents, including accreditation and observer applications may be submitted in English or in another language. In the latter case, the documents shall be accompanied by an English version. Members with the ability and the resources to do so are encouraged to translate proposed resolutions and other Assembly documents such as the Assembly Rules and Procedures.

Privacy Commissioner for British Columbia, and la Commission d'accès à l'information du Quebec (The Canadian Authorities) worked in concert to address the global privacy concern of Facial Recognition Technology (FRT) using a variety of compliance tools. Specifically, they carried out a series of enforcement actions in both commercial and law enforcement contexts of FRT, examining both purveyors and users. We amplified the impact of this enforcement through the concurrent release of joint draft guidance for consultation - on the use of facial recognition technology by police forces.

**b. Please provide a full description of the initiative** *(no more than 350 words)*

Our Offices took a strategic coordinated enforcement approach to examine FRT from three relevant angles: (i) purveyors (Clearview AI), (ii) law enforcement users and (iii) commercial users.

Four Canadian DPAs[2] jointly investigated Clearview AI, a major global FRT purveyor. We concluded that Clearview could not scrape personal information without consent, simply because the images were accessible on the internet. Further, we found Clearview's FRT services to contravene Canadian privacy law[3] - constituting mass surveillance, resulting in millions of individuals effectively being in a continual police line-up even though they had never been implicated in a crime. We were successful in having Clearview exit the Canadian market, and we continue to pursue Clearview's deletion, and cessation of collection, of Canadians information.

In a complementary investigation, the OPC concluded that it was a contravention of the federal Privacy Act for the Royal Canadian Mounted Police (national police) to collect personal information using Clearview that had been collected in violation of laws Clearview was subject to. We also concluded the national police needed to assess against common law constraints on the authority of a police body when deciding how to use FRT. The national police agreed to implement extensive new measures to track and control new technologies including FRT, and assess private purveyors it uses for compliance with Canadian privacy laws.

Finally, in a joint and related investigation, the Canadian authorities investigated the use of FRT technology by the largest shopping mall operators in Canada.[4] The malls used FRT to analyse images of shoppers via inconspicuous cameras with the objective of determining their age and gender for marketing purposes. In one case, we concluded that the operator required informed opt-in consent for this practice. The Commission d'accès à l'information du Quebec also made observations on privacy issues regarding another operator. Both operators ceased using the technology. In the aforementioned joint investigation, we discovered and addressed the previously unknown retention of 5 million biometric profiles by the operator's FRT purveyor, successfully obtaining agreement to delete them.

[2] Ibid.

[3] Appropriate/Reasonable Purposes (Necessity/Proportionality)

[4] Cadillac Fairview (using Mappedin, a purveyor of FRT) – Joint Investigation by the OPC, OIPC-AB and OIPC-BC; Ivanhoé Cambridge – Investigation by the CAI. While these investigations were conducted separately, our Offices shared information as appropriate.

To amplify the effectiveness of these enforcement decisions and to promote General Compliance, the Canadian Authorities concurrently issued draft joint guidance for consultation with police bodies on the use of FRT. The enforcement work and guidance were highlighted together through a special report to Canada's federal parliament.

**c. Please explain why you think the initiative deserves to be recognised by an award** *(no more than 200 words)*

This is an example of regulators working together strategically in enforcement to address an important emerging global privacy risk from multiple angles - promoting broad-based compliance. It represents an expedient, effective, and resource efficient approach that produced holistically superior results for the privacy protection of individuals. Of specific note:

- the coordinated investigations of commercial use of FRT achieved complementary positive results without duplication of effort.
- the Canadian Authorities combined resources (as well as different enforcement powers) to complete a joint investigation of Clearview - issuing meaningful findings and securing Clearview's exit from Canada in less than a year.
- the Authorities strategically issued enforcement decisions relating to both the purveyor-side (Clearview) and user-side (national police, mall operators) – ensuring awareness of obligations across the board.
- the collaborative enforcement actions amplified our messaging with: nation-wide and international coverage, engagement of our federal Parliament, and media coverage reaching an estimated 33 million people globally.

These enforcement actions provided invaluable support as our Offices advocate for stronger privacy laws - bringing emphasis and attention to concurrently released joint draft guidance for consultation on police use of FRT – highlighted with the enforcement actions in a special report to Canada's federal parliament.

Finally, these investigations are helping inform the work of other international authorities and networks, as we are sharing lessons learned with the GPA's FRT working group, GPEN, APPA and the IEWG.

**d. Please include a photograph or image, if you wish** *(This will be published with your entry on the GPA website. The image can be pasted into the box below, be sent as an attachment or a link may be provided)*

N/A

**e. Please provide the most relevant link on the authority's website to the initiative, if applicable** *(The website content does not need to be in English)*

**Clearview**
Report of Findings: Joint Investigation into Clearview AI, Inc
OPC Press Release – Clearview AI

**Cadillac Fairview**
Report of Findings: Joint Investigation into Cadillac Fairview
OPC Press Release – Cadillac Fairview

**Ivanhoé Cambridge**
Ivanhoe Cambridge: Closure Letter (French Only)

**Facial Recognition Technology Guidance to Law Enforcement**
Notice of Consultation
Draft Privacy Guidance on FRT to Police Agencies

**Royal Canadian Mounted Police**
Special Report to Parliament: Use of FRT by the RCMP and the way forward
OPC Press Release - RCMP

**f. Please provide any other relevant links that help explain the initiative or its impact or success** *(e.g. links to news reports or articles):*

**Clearview**
Clearview AI's Facial Recognition App Called Illegal in Canada – New York Times
Canadian Regulators Say Clearview Violated Privacy Laws – Wall Street Journal
U.S. technology company Clearview AI violated Canadian privacy law: report - CBC
Clearview AI broke Canadian privacy laws by selling software to police, watchdogs say – Globe and Mail

**Cadillac Fairview**
Mall real estate company collected 5 million images of shoppers, say privacy watchdogs - CBC

**Ivanhoé Cambridge**
Caméras à Place Ste-Foy : une enquête pour atteinte à la vie privée – Radio Canada (French Only)

**Royal Canadian Mounted Police/Special Report to Parliament**
RCMP's use of facial recognition tech violated privacy laws, investigation finds – CBC
Privacy watchdog says RCMP broke law in using facial-recognition tool – Globe and Mail
La police canadienne a utilisé la reconnaissance faciale de façon illégale - Le Figaro avec l'Agence France-Presse (French Only)
Canada police broke law with facial recognition software, regulator finds - Reuters