Facial Recognition
Parliamentary Appearance – House of Commons Standing Committee on Access to Information, Privacy and Ethics
April 28, 2022

OPENING REMARKS

- Good afternoon Mr. Chair and Honorable members of the Committee, I am grateful for the opportunity to speak with you today on this important issue, which I hope will inform your study into the use and impacts of facial recognition technology.

- As a concept, facial recognition has been used in policing for as long as policing has existed. At its root, facial recognition is the basis of eye witness testimony, police line ups, and "mug" shots, and relies on the ability of a witness to compare various images of people's faces to the person they saw, based on the witness' recollection.

- This technique continues to be employed today to support criminal investigations and the RCMP maintains a national database of lawfully collected criminal record information, including photographs, fingerprints and other biographical information for this purpose.

- With advanced artificial intelligence and machine learning technologies, we are seeing the growth of new biometric analysis tools that allow for a more quantified comparison or matching of images and video, such as Facial Recognition Technology or FRT. The unprecedented increase in the prevalence of digital technology in the daily lives of Canadians also means that there is an increasingly abundant amount of digital imagery available to criminal investigators.

- FRT offers a new and significant opportunity for all law enforcement, particularly in an organization with diverse mandate, such as the RCMP with applications extending from the identification of the victims of child sexual exploitation, to the investigation of violent crime, FRT has the potential to greatly augment existing investigative techniques.

- This said, the RCMP is firmly of the position that this technology must not be used indiscriminately. FRT should only be used in a targeted and time limited fashion for a specific purpose and in a manner consistent with *Charter* and the Canadian privacy protection framework. This technology should not be used to collect personnel information from Canadians without specific cause.

- Despite the fact that FRT has been around for a relatively long time, it should still be considered an emerging technology. Systems developed to-date have been known to suffer from inaccuracies and bias that can result in false positive results. For this reason, the RCMP has never used the results of an FRT match as confirmed identity, instead requiring trained examiners to assess possible matches to determine their veracity.

- Simply put: FRT can produce an investigative lead but trained investigators still need to determine and confirm relevance and accuracy in the course of their investigation, and corroborate an identification through other investigational means.

- While new technology can enhance our ability to conduct investigations more efficiently and effectively, we recognize that our primary obligation is to ensure all policing activities are lawful and conducted in accordance with the *Charter*, *Privacy Act* and all other relevant laws, regulations and policies.

- From October 2019 to July 2020, the RCMP made limited use of a facial recognition technology, Clearview AI, to support our National Child Exploitation Crime Centre, or NCECC, with the identification of victims of online child sexual exploitation.

- I would first like to acknowledge that our initial disclosure of the use of this tool was incomplete. It was not intended to be so.

    - When initially responding to media enquiries and the Privacy Commissioner, it was not commonly known that, across such a large organization as the RCMP, a limited number of programs had begun using Clearview AI, whether with a paid licence or on a trial basis. We responded in error to the Privacy Commissioner and early media enquiries based on an incomplete survey of RCMP program areas.

    - Once we became aware of the broader use of Clearview AI, a more fulsome survey of all RCMP programs and Divisions was made to understand the full extent of the use of Clearview AI within the RCMP. We also immediately notified the Office of the Privacy Commissioner (the OPC).

- The use of Clearview AI by the RCMP was not widespread. The RCMP had a total of twenty (20) licences for Clearview AI – two (2) paid and eighteen (18) trial licences available at no cost only to law enforcement agencies.
    - 65% of the twenty licenses (13) were used for victim identification by the NCECC, seven (7) were trial licences associated with Internet Child Exploitation units in Divisions across the country.

- As you are aware, the OPC conducted an investigation on the RCMP's use of Clearview AI. The RCMP has worked cooperatively with the Privacy Commissioner on this investigation and we welcomed the recommendations of their report.

- The Privacy Commissioner made a number of recommendations for improvements to our current training and operational processes, including the creation of a centralized and standardized process for identifying, tracking, assessing and reporting new technologies that make use of personal information.

- We have fully accepted the recommendations of the Privacy Commissioner and view their implementation as an opportunity to strengthen our existing policies and processes.

- As a key part of our response to the OPC, we have established the National Technology Onboarding Program (or NTOP), to centralize the tracking of new operational tools being used or considered for use across the RCMP. NTOP establishes a standardized process for the implementation of developed or procured technologies and services, including legal, technical and policy assessments, GBA+ and privacy analysis. This is a significant undertaking, but we are hopeful that NTOP will be fully operational this fall. We continue to work closely with the OPC as we implement these recommendations.

- We recognize that technology can and does outpace legislation and regulation. For some existing biometric tools, such as fingerprints and DNA, the government has developed strong legislative and regulatory frameworks that delineate how federal agencies are permitted to use these tools. However, as newer techniques have become available, particularly those involving the use of digital information and media, the legislation has not kept pace, leaving a void that departments and agencies have been left to fill.

- The use of biometric tools that leverage images and videos (such as facial recognition, gait analysis, and voice print analysis) could be significant tools that benefit criminal investigations and, help to bring justice to victims of crime. With NTOP we hope the RCMP can demonstrate its commitment to transparency, accountability and leadership across law enforcement on how to identify and work with our government partners, including the Privacy Commissioner, to implement new solutions.

- Thank you. I am happy to answer any questions you might have.