ETHI Opening Statement – Patricia Kosseim

May 2, 2022

656 words; check against delivery

- Good morning, and thank you for inviting me to speak today.

- While I've previously had the pleasure of appearing before this Committee, I am speaking today in my current role as Information and Privacy Commissioner of Ontario. Joining me is Vance Lockton, Senior Policy and Technology Analyst with my office.

- I would like to build on the remarks you've just heard from Commissioner Therrien.

- While Canada's Privacy Commissioners recommend the adoption of a comprehensive statutory framework to address the use of facial recognition technology in the law enforcement context, we also recognize that some police agencies are already using, or considering using, facial recognition technologies, for example, to support the investigation of serious crimes or help locate missing persons.

- As such, we have issued guidelines to guide law enforcement agencies in the interim and help mitigate against potential harms until a new statutory framework is put in place.

- I would like to emphasize 5 key elements of the guidelines.

- **First**, before using facial recognition for any purpose, police agencies must establish that they are lawfully authorized to do so.

- This is not a given, and cannot be assumed. Facial recognition relies on the use of sensitive biometric information. Police should seek legal advice to confirm they have lawful authority either at common law or under statute *specific* to their jurisdiction. They must also ensure they are Charter-compliant and their purported use is necessary and proportionate in the circumstances of a given case.

- **Second**, police agencies must establish strong accountability measures.

- This includes designing for privacy at every stage of a facial recognition initiative and conducting a privacy impact assessment (PIA) to assess and mitigate risks in advance of implementation.

- It also involves putting in place a robust Privacy Management Program, with documented policies and procedures for limiting the purposes of facial recognition, robust systems for logging all related uses and disclosures, and clearly-designated roles and responsibilities for monitoring and overseeing compliance.

- Such a program must be annually reviewed for its continued effectiveness; it must be supported by appropriate training and education, and ensure that any third party service providers also comply with all related privacy obligations.

- **Third**, police agencies must ensure the quality and accuracy of personal information used as part of a FR system to avoid false positives, reduce potential bias and prevent harms to individuals, groups and communities.

- Ensuring accuracy involves conducting internal and external testing of the FR system for any potentially discriminatory impacts, as well as building in human review to mitigate risks associated with automated decisions that may have significant impact on individual rights.

- **Fourth**, police agencies should not retain personal information for longer than necessary. This means destroying probe images that do not register a match, and removing face prints from the face database as soon as they no longer meet proper criteria for continued inclusion.

- **Fifth**, police agencies must address transparency and public engagement.

- Direct notice about the use of facial recognition may not always be possible in the context of specific police investigations. However, program-level transparency *is* possible – such as publishing the agency's formal policies on the use of FR, a plain-language explanation of their FR program, and a summary of their PIA.

- But communication with the public shouldn't just be one-way – key stakeholders, particularly representatives of over-policed groups, should be consulted in the very design of the facial recognition program, including during the PIA process. Given the particular importance of reconciliation in Canada, this must include input from local Indigenous groups and communities.

- These are but a few of the measures set out in the guidance.

- To re-iterate, although we believe these guidelines represent important risk mitigation measures, ultimately we recommend the establishment of a comprehensive statutory regime governing the use of FR by police in Canada.

- Clear guardrails with force of law are necessary to ensure police agencies can confidently make appropriate use of FR technology, grounded in a transparent framework capable of earning the public's enduring trust.

- Thank you.