OBA Submission on Privacy Guidance on Facial Recognition for Police Agencies

Submitted to: Information and Privacy Commissioner of Ontario

Submitted by: Ontario Bar Association

Date: October 15, 2021

ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

L'ASSOCIATION DU BARREAU DE L'ONTARIO
Une division de l'Association du Barreau canadien

Table of Contents

I. Introduction

The Ontario Bar Association ("**OBA**") appreciates the opportunity to provide this submission in response to Canada's federal, provincial and territorial privacy protection authorities' consultation on guidance for police agencies with respect to their use of facial recognition ("**FR**") technology.

Established in 1907, the OBA is the largest volunteer lawyer association in Ontario, with over 16,000 members who practice on the frontlines of the justice system and who provide services to people and businesses in virtually every area of law and in every part of the province.

Each year, through the work of our 40 practice sections, the OBA provides advice to assist legislators and other key decision-makers in the interests of both the profession and the public and delivers over 325 professional development programs to a diverse audience of over 16,000 lawyers, judges, students and professors.

This submission was prepared by members of the OBA's Privacy Law and Access to Information Section, Information Technology and Intellectual Property Section, Constitutional, Civil Liberties and Human Rights Section and the Criminal Law Section.

II. Overview

We commend the Privacy Commissioners for their important work on drafting guidelines for the use of FR technology for police agencies. Ensuring the balance between public protection and privacy rights of residents of our province is an important and worthy undertaking.

For the purposes of the public consultation, this submission focuses on general recommendations for establishing guidelines for the use of FR technology by police agencies and also provides specific recommendations in response to questions posed by the Commissioners. Our members believe our submission will help the Commissioners more effectively and efficiently balance the competing interests of public safety and privacy rights.

III. General Recommendations

The OBA recommends taking a restrictive approach to facial recognition technology given the privacy interests at stake, concerns over the technology's reliability, and the need to regulate "big data" in a clear and consistent manner. While many investigative techniques have been utilized for many years - for example, manual review of CCTV videos in public places or circulation of photos to the public asking for identification - the sheer power of FR software (and its inherent frailties) changes the nature of what we have previously understood to be a basic right to move about society anonymously. Thus, the normative expectations shift with FR technology, and as the s. 8 Charter framework is normative-based, clear guidance and regulation at the outset is needed.

At a conceptual level, restrictions must be placed at multiple and progressive "check points" concerning the *collection*, *access*, *use*, *retention* and *notice* of FR data. No one measure ought to be relied on to mitigate the risks. Rather a multi-faceted approach is required. Limits on the collection of data mitigate data

retention issues. What use can be made of FR technology may also impact what data can be collected. Limiting access to FR data restricts potential uses during more routine law enforcement. Strong retention policies that favour permanently deleting data when the purpose for which its collection is completed (e.g. at an airport check in) minimizes the risk of inappropriate use and access down the road. The OBA is pleased to see such an approach being adopted and commends the draft guidelines for their thoroughness and comprehensiveness.

As a general comment, the draft guidelines repeatedly refer to a "FR initiative". It is unclear what this means. Does that mean a particularized police investigation in response to a specific alleged offence? Does this mean the police creation of a more general database to be trolled for "hits" akin to the DNA National Databank? Does this mean creating linkages to pre-existing databases (e.g. driver's licence photos)? If yes, under what circumstances?

These are important questions as the OBA believes more specific guidance must be provided to law enforcement if the proposed guidelines are to be practically implemented and to have the effect of ensuring appropriate mitigation of the privacy risks involved. In the absence of clarification, the limits on the technology may erode over time as law enforcement finds new and innovative uses of the technology ultimately leaving regulation to the common law post-hoc.

1. *Collection*

One of the key questions for the use of FR technology is how the information is cultivated. We recommend that police authorities limit the data sources that can be used for facial recognition by law enforcement.

The presumptive approach ought to be consent-based. Generally, the underlying reference images should only be collected where there is transparency and express consent for a law enforcement purpose. Where an individual has not consented to providing an image for FR technology, it should only be used in cases where those images are already routinely and lawfully collected for law enforcement purposes when the individual's privacy interest is balanced against the public interest in enforcing laws. For example, the use of mug shots may be an instance where FR may be appropriate due to the prior assessment of the expectations of privacy.

Commercial use and development of FR technology in Canada has primarily been restricted to situations when individuals provide express consent. FR technologies have been used by police forces across the country, but initial research has found no clear law outlining when and where it can be used.

We strongly urge police agencies to avoid the collection of images from the Internet. Photographs provided for social media, for example, have been provided for a distinct purpose, and not for any law enforcement purpose. In addition to the privacy considerations involved in using photographs gathered from the Internet, we urge police agencies to consider the potential for images shared online to be inaccurate (e.g., "filters" or other edits may have been applied to the images, eg. digital alteration by programs such as Photoshop).

2. *Access*

Biometric data is biologically unique, and therefore heightened security is required to prevent inappropriate access. Data can be stored in numerous forms, most frequently though through numeric templates. It can easily be transferred digitally through downloads, etc. Increased security is thus required for storage

of relevant data to minimize threats to hacking and illegal access to the data which could be used for unintended purposes such as for profit by companies, or to violate privacy rights of Ontario residents.

Police agencies should not be able to store new information collected on individuals who have not been found guilty of an offence, and information about such people should be destroyed afterwards. For example, if an individual was at the airport to board an outboarding flight, their face may be scanned by FR technology, but once cleared through security, that information ought to be destroyed by law enforcement agencies.

Police agencies ought to be prohibited from disclosing, selling, leasing or trading the data to other organizations, companies or countries without proper legal justification. For example, the data captured at an airport could help marketers determine which air travelers are visiting which retail stores and their purchasing habits. The sensitive information would also be of value to other countries or border agencies who engage in wide-spread surveillance of their citizens. Such activities are not within the mandate of police agencies and may not be justifiable under s.1 of the Charter, if a challenge should ever arise as a result of such activity.

3. *Use*

We urge police agencies and individual officers to be restricted from the unfettered use of FR technology. Restrictions must be placed on what use can be made of the technology. We recommend two restrictions. First, the technology must be limited to specific instances of alleged criminality involving specific individuals whether identified or not for which reasonable suspicion exists. The experience of cell phone "tower dumps" shows how the private information of innocent parties can be captured in police investigations.

Second, the results can only be used for investigative purposes and should not be admissible as substantive evidence in court. An analogy is to a roadside screening device for impaired driving; it can provide the grounds to arrest a person but cannot be used as substantive evidence of proof of blood alcohol content over the legal limit.

The difficulty with more substantive evidentiary use of FR technology is that it can be difficult to challenge in court as it often involves the use of complex, proprietary algorithms. Many accused today are unrepresented or do not otherwise have the means to understand the technology, much less the resources to challenge it. In addition, many companies that offer such technologies are unwilling to publicly disclose precisely how their algorithms work, as to do so may harm their intellectual property interests. Accordingly, ensuring the accuracy of the technology and identifying any flaws, is more difficult and poses an additional burden on accused.

We recommend requiring full disclosure to accused persons of the particulars of any FR technology if it has been used with a view to criminal or other judicial proceedings. Where requested, we believe the algorithm, any training data, and records of accuracy should be available to defendants, or the subject of investigative proceedings based on FR technology. Care will have to be taken to address any concerns (to the extent possible) raised by technology providers regarding the confidentiality of their algorithms and systems operations (*e.g.*, where the FR technology involves confidential information, trade secrets, or as yet undisclosed or unpatented innovations).

Limited use is particularly important until there is greater accuracy. The current technologies have been shown to have inherent bias against certain minority groups, thereby yielding discriminatory results. For example, some FR software falsely misidentifies Black and Indigenous individuals more than white people due to algorithm bias.[1] The National Institute of Standards and Technology in the United States found the problem was so significant that FR technology was about 5 times more likely to misidentify Black women than white women.[2] FR technology can also have issues identifying other races, females compared to males, different ages and transgender individuals. Failing to address this accuracy issue will continue the perpetual issue of overrepresentation in the justice system of Black and Indigenous individuals and surveillance of the same. The potential harm is of such significance that at least 13 cities in the United States have banned the use of FR technology. In April 2021, the European Commission released a regulatory proposal identifying FR technology as a "high-risk application" with particular concern that its use "may lead to human rights abuses in the absence of robust governance mechanisms."[3] As a result of these issues, we propose that there be clearly established accuracy prior to the implementation of any FR technology for police purposes.

Further, to ensure accountability and evidence-driven regulatory reform, use of the technology should be transparent in terms of how and when it is used and the statistics it produces. For example, how often are false matches produced, how many times has the technology resulted in prosecutions. A regulation or law would help ensure accountability. In New York City, the *Public Oversight of Surveillance Technology Act*, was introduced to increase transparency and oversight of the use of FR technology. The Act was introduced following the use of FR technology with algorithm bias by police agencies resulting in a lawsuit. Ensuring accountability of the technology prior to its use is key to ensure against human rights abuses.

4. Retention

Restrictions must be placed on data retention with strict controls on who has access, how long data is held, and providing options for individuals to request and/or verify deletion. Accountability for breaches of protocol must be built into any regime. One helpful distinction is records versus evidence and the distinct rules that may apply to each.

We agree with the draft guideline's approach to deleting data that is no longer necessary to fulfill the purpose. However, again, this begs the question of the scope of an "initiative" and when the purpose would be "fulfilled". Clearly, images captured in a fleeting manner to verify identity (e.g. automatic airport kiosk) ought to be deleted promptly. However, if "initiative" is meant to be a specific investigation then images collected pose a challenge, as often times they can become relevant for post-conviction review. Likewise, if the "initiative" means the creation of a stand-alone database or use of an existing database (e.g. mug shots) then that further may change retention polices if an individual is subsequently acquitted or the charges are stayed or withdrawn. How that is managed with FR technology is unclear. More guidance on these considerations would provide significant assistance.

[1] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, December 19, 2019
[2] *The Best Algorithms Still Struggle to Recognize Black Faces | WIRED*, July 22, 2019
[3] *This is Best Practice for Using Facial Recognition in Law Enforcement*, October 5, 2021

5. Notice

The use of and how notice will be used should be clarified and defined. On many occasions, individuals may only read a notice that they are being recorded [Camera Capturing]. However, the options are limited, as they either must refrain from attending at the premises or be deemed to have consented to their images being captured and recorded.

IV. Specific Recommendations

With the above recommendations in mind, we have provided below specific recommendations in response to questions outlined in the consultation document. Based on our members' knowledge of the applicable legal principles and their thorough understanding of privacy, intellectual property and information technology, constitutional and human rights, and criminal law, we are providing feedback on specific but not all of the consultation questions.

1. Ensuring police agencies' use of FR technology is lawful and mitigates privacy risks

The guidance from the Privacy Commissioner is unlikely standing alone to sufficiently mitigate the privacy risks posed by police use of FR. The value of the guidance is in providing a framework within which the courts, legislature, police departments, and other judicial/societal actors can understand the risks and measures to mitigate those risks.

However, as indicated above, the policy document needs to differentiate more specifically between the various law enforcement FR "initiatives" as different considerations arise depending upon the scope of the initiative(s). In essence, the draft guidelines need to be much more specific to have the intended effect of ensuring lawful use and risk mitigation. Indeed, they are quite specific and directive in some places with language such as "should not" or "shall not" or "should".

The OBA appreciates the need to balance generality of guidance versus specificity for individual cases in an overarching policy document, however particular attention ought to be paid to the following:

- Investigative uses of the technology (for instance, identifying suspects from surveillance to ultimately conduct independent investigation of those suspects or obtain a warrant) versus substantive use as evidence in a court proceeding as different disclosure obligations, procedures, and retention policies may apply - ultimately the OBA recommends not using FR technology for substantive evidentiary purposes;

- Whether the FR initiative seeks to establish a reference database, create linkages with existing databases, or is purely limited to specific incident of alleged criminality - again, unique considerations apply depending on which and police ultimately will need more guidance surrounding each potential use and each cannot be lumped together into a general policy document;

- Circumstances in which prior judicial authorization may be required, for example to cross-reference with a pre-existing database (e.g. health card photos, employee database, etc.) or when express consent has not been previously provided for the image to be used for law enforcement purposes -

in other words, the policies may have to be different depending on the source of the data as the privacy considerations can change - this must be specified in greater detail lest law enforcement treat each as subject to the same policy framework; and

- Stressing the need for heightened restrictions the more invasive the use of the technology - for instance, fleeting capture and deletion of an image to verify someone arriving at an airport against their passport versus populating a reference database for comparisons in specific instances of alleged criminality - particularly for whether those reference databases could be populated by radicalized or marginalized individuals in a specific community (e.g. gang investigations) – an analogy to this can be found in the practice of "carding".

Failure to provide guidance in these areas means that much will be left to after-the-fact case law analyses and an opportunity will have been missed to provide guidance at these initial states of FR technology implementation.

3. Are the recommendations in the 'accuracy' section sufficient to help ensure police agencies meet their accuracy obligations in FR initiatives?

The recommendation in para. 81 should be supplemented by making the results of the independent external testing publicly available. Realistically, it is most likely to be parties independent from law enforcement who will hold law enforcement agencies accountable when FR systems fall below acceptable levels of accuracy.

Further, consideration ought to be given to the data sources that are used to populate any reference database for the FR initiative. This is highlighted at para. 78, however consider cases in which the database may be created of members of a particular racial and/or geographic community. The danger is of rounding up the "usual characters" or of further perpetuating stereotypes of gang involvement or criminality. The guidelines as drafted cannot correct for this. The OBA recommends at the very least a blind procedure of human review in such cases whereby an officer not involved in the investigation or who has familiarity with the suspects conducts an independent human review to mitigate the risk of confirmation bias. This could be buttressed by the use of control face samples similar to the procedure used for a photo line-up.

7. Feedback on the current use of regulation of FR technology use by police

In our view, the existing Canadian law is not properly suited to regulate FR, and a statute and/or regulations should be created which is specifically tailored to the concerns raised by FR. As noted above, other jurisdictions such as New York have begun to introduce legislation specific to FR and other biometric data.

Again, these guidelines present a chance to build in strong protections at the front end rather than for policy to come through judge made rules or on an ad hoc basis. Creating a new regulatory/statutory framework also opens the door to legislative study and structured public consultations.

Unlike fingerprinting or DNA collection, images collected for the use in FR can easily be collected remotely, and without the individual's knowledge or consent. We believe that there must be specific restrictions implemented to limit the collection and use of biometrics. We note that the *DNA Identification*

Act, S.C. 1998, c. 37, has similarly been specifically drafted to create a principled approach to the use of DNA in law enforcement investigations.

It also creates the opportunity for creation of an oversight body and a legal requirement of mandatory periodic review.

8. Protections for individuals whose biometric information is captured

The information available as to what kind of biometric information is retained in faceprint databases is limited and it is prejudicial to certain racial groups, namely those from the Black community and other racialized groups. The analogy is often drawn between faceprint and mugshot databases and DNA banks. However, notice is generally given to individuals who are sentenced prior to providing DNA information in DNA banks. It does not appear that any notice is provided to individuals whose faceprint data is captured. While policing agencies may allege they are permitted to use identification photos (i.e. mug shots) in such databases, this does not alleviate the fact that no notice was provided. It is too early in the consultation stage to say what kind of protections should be provided but at minimum, notice ought to be provided to individuals as noted earlier.

9. Limitations on the use of Collection of Face Prints

The analogy often used in the use of FR is that police already use similar databases and this is an extension of those databases, DNA banks is one example of this, as noted above. However, DNA banks are limited in their application and there are procedural protections in place that protect the Charter rights of individuals facing allegations; DNA orders, more appropriately, also come at the end of a criminal proceeding when a finding of guilty or conviction is entered. Similarly, police use of FR should not occur without express authorization and procedural protections in place similar to DNA banks, which have been upheld as constitutionally sound. There is information available that confirms the police have used FR without authorization and this causes deep concern as to how FR information is being presently retained beyond non-conviction situations.

10. General Considerations of the use of FR Technology by Police

In response to the final question of the consultation, we recommend three key considerations for the FR technology guidelines for police agencies ("**Guidance Document**"); oversight, a reporting mechanism and purpose limitations.

Oversight: What powers will the Commissioner have to oversee the implementation of the guidance?

The Guidance Document provided by Canada's federal, provincial and territorial privacy protection authorities can have limited effectiveness unless it is followed up with oversight from the privacy protection authorities. The proposed guidance recommends that law enforcement agencies implement effective accountability measures, including, but not limited to, logging all uses of FR. It would be helpful for the privacy protection authorities to signal to Canadians what, if any, compliance and enforcement activities are planned to ensure that law enforcement agencies are, in fact, using FR in compliance with the proposed guidance and Canada's privacy laws. Will Canadians be expected to file complaints with Canada's privacy

protection authorities or will these authorities take proactive steps to ensure compliance by law enforcement agencies?

Lack of a Mandatory Reporting Mechanism

Sections 88-89 of the Guidance Document suggest the implementation of a set of *'administrative, technical, and physical controls'* for managing access to and use of data and FR software, which internal controls seem to culminate in informing and obtaining approval from senior management. Short of introducing a requirement similar to PIPEDA's mandatory data breach reporting, whereby law enforcement must report incidents of abuse of power pertaining to collection and use of personal information and FR technologies, this guidance becomes easy to ignore and this deficiency cannot be cured by the discretion to order a Privacy Impact Assessment. Some form of a mandatory reporting mechanism is therefore encouraged.

Purpose Limitation: Database Creation, FR Software Training, and Risk of Bias

The Guidance Document provides that *'police agencies must ensure that personal information is only used for the purpose for which it was collected, or a purpose consistent with that purpose.'* Two issues seem to arise from this recommendation. First, the number of citizens providing consent to have their biometric/personal data stored in a similar (faceprint) database for future use in a police investigation is realistically very low. Where citizens 'consent is not required because such data has been obtained pursuant to the police's demonstrated lawful authority or a warrant, the said data cannot be used for other (non-consistent) purposes, which is homogeneously agreed upon by privacy laws and jurisprudence, and is in line with the Guidance Document. It is unclear, however, if a *'purpose consistent'* with the purpose, based on which such data was collected, includes training FR software for the related investigation. This leads to the second issue; without a sufficient (permissible) data volume to train FR software, the risk of perpetuating bias and leading to discriminatory outcomes seems inevitable, as it is proven by recent bans implemented by 'Big Tech' over the use of their FR tools by the police. Therefore, more clarity is required on what constitutes a *'consistent'* purpose, as described in the Guidance, and the steps required to properly train FR software with permissible data, abiding by privacy laws, to eliminate the risk of false positives and biased outcomes.

V. Conclusion

In closing, we believe that the OBA recommendations, based on our members' knowledge of the applicable legal principles and their thorough understanding of areas of law that touch upon the use of FR technology by law enforcement agencies will help improve the approach to the guidance document you are looking to provide for the sector.

Thank you for taking the time to review the submission. We hope you find the feedback from the OBA helpful and informative in your next steps. We look forward to continued dialogue on the development of this important document as you seek to balance public safety with individual privacy rights.