THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

February 14, 2024

Via email: OPC-CPVPconsult1@priv.gc.ca.

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec KIA 1H3

Re: New draft guidance on biometric technologies (OPC)

I am writing on behalf of the Privacy and Access Law Section of the Canadian Bar Association (CBA Section) in response to the public consultation on new draft guidance of biometric technologies launched by the Office of the Privacy Commissioner of Canada (OPC) on October 11, 2023. The draft guidance provides information on privacy obligations, considerations, and best practices for handling biometric information. It is divided into two documents: *Draft Guidance for processing biometrics – for organizations* and *Draft Guidance for processing biometrics – for public institutions*.

The CBA is a national association of 38,000 lawyers, Québec notaries, law teachers and students, with a mandate to promote improvements in the law and the administration of justice. The CBA Section comprise lawyers with an in-depth knowledge of privacy and access law

The CBA Section responses to the survey questions in the consultation are limited to the 1,000 word maximum.

1. **Identifying appropriate purposes:**

Are there specific uses of biometrics that should be considered inappropriate? Should we define these no-go zones in the guidance?

The CBA Section agrees that the use of biometrics should be reserved for use-cases where the use is appropriate and balanced considering all the surrounding circumstances. The framework set out in the draft guidance, following *Turner v Telus,*[1] is comprehensive, coherent and workable.

With respect to no-go-zones, the CBA Section is mindful that technologies, use cases and the reasonable expectations of individuals all evolve. The OPC should be cautious about baking in categorical prohibitions that are not directly connected to the underlying circumstances. That said, any use of biometrics that results in a violation of another law, such as human rights laws, is unlawful. The OPC's final guidance should include a clear statement that use of biometrics may involve other laws which are to be considered to decide whether the use of biometrics is appropriate.

[1] 2005 FC 1601

2. Limiting collection:

We state in the guidance that you must seek to keep the biometric template in the individual's control but acknowledge this won't always be possible. Are there other suggestions for biometric template models or other practices to limit an organization's collection?

It is important to recognize that appropriate methods and practices are highly contextual and that the "correct" approach will depend on the circumstances. The CBA Section makes the following recommendations:

- Change "Use authentication before identification" to "Favour authentication over identification" in the "You Must" column of the Limiting collection section. This proposed wording is less likely to be misinterpreted as a potential process (e.g., authenticate, then identify).
- According to the OPC's *Personal Information Protection and Electronic Documents Act* (PIPEDA) Report of Findings #2010-007 case summary: Focus less on the organization and more on the issue and solution(s) at the heart of the investigation. This comment applies across the guidance – it is unnecessary to identify investigated organizations in the guidance itself. The lessons learned from the investigations should be the emphasis.
- Under "Not copy identity document" of the "You Must" column, the second paragraph should be qualified. While it is the exception, there may be circumstances where it is appropriate to not "immediately" delete copies of identity documents. Given that identity documents may be copied in certain cases, the requirement to "Not copy documents" should be moved under the "You should" column.
- Consider noting that filtering tools/technologies may assist organizations and government institutions from collecting unwanted or unneeded personal information submitted by individuals. Organizations should also review their collection practices from time to time to ensure only necessary personal information is collected.

Do you think multi-modal biometrics (systems that use more than one biometric identifier) could be necessary in some circumstances to offer adequate safeguarding, or should these generally be considered an over-collection?

The CBA Section agrees that yes, multi-modal biometrics may be appropriate under certain circumstances, but this will be context dependent. Organizations should be urged to limit the number of biometric identifiers they collect, but whether the use of a multi-modal system is an over-collection will depend on the context.

3. Safeguards:

Safeguards are particularly important given the sensitivity of biometric data. Are there additional safeguards specific to biometrics over and above those proposed in the guidance, such as technical methods, that we could suggest?

The CBA Section recommends fraud detection approaches to biometrics that do not directly identify an individual. The approach to safeguards will change constantly as technology evolves and the recommendations should reflect that fact.

Some recommendations may be commercially impractical or unfeasible. The cost of storing access logs for any period can be incredibly high. Funding a separate storage instance for biometrics may also be impractical or unworkable.

We believe most organizations rely on third-party service providers for any form of biometric solution. The guidance presumes that the organization has control over the build out of the technology, which generally it does not. Most third-party service providers are US- or EU-based and the regulators in these jurisdictions have generally adopted a principle-based (versus a prescriptive) approach to determining the appropriate safeguards to put in place. To promote international harmonization of privacy laws, the CBA Section recommends that the guidance refrain from adopting a prescriptive approach, granting organizations (and third-party service providers) the flexibility to assess their circumstances and determine the best measures to implement for each of their biometric initiatives.

4. Accountability:

Are there requirements in the guidance that should be specifically directed towards vendors/manufacturers of biometric equipment, and the organizations that choose to use such equipment for the collection of biometric data?

The CBA Section relies on basic principles for accountability purposes. The 10 Fair Information Principles listed in Schedule 1 of PIPEDA ought to be followed by all organizations. They are:

- Accept responsibility for personal information under its control;
- Designate at least one representative to be accountable for the organization's compliance with the 10 principles set out in Schedule 1 of PIPEDA;
- Make the identity of the designated individual(s) known on request;
- Protect all personal information in the organization's possession or custody, including information that has been transferred to a third party for processing;
- Use contractual or other means to ensure a comparable level of protection while personal information is with a third party for processing;
- Develop and implement policies and practices to uphold the 10 principles set out in Schedule 1 of PIPEDA including:
- Implement procedures for protecting personal information;
- Establish procedures for receiving and responding to complaints and inquiries;
- Train staff and communicating information to staff about the organization's policies and practices; and
- Develop information to explain the organization's policies and procedures.

Every company must have a robust breach plan that outlines its breach reporting protocol to ensure timely reporting of any breach that poses a real risk of significant harm to individuals.

A third-party can handle breach reporting but account for privacy of client information. This is integral to biometric protection of information and keeping client identity safe. Ensuring full audit of the third-party provider is an additional and recommended suggestion for all companies to bear in mind.

5. General:

Are there any other outstanding areas of regulatory uncertainty that this guidance can help clarify? If so, what are they and why do you think they should be included?

D. Additional comments

Please provide any additional comments you'd like to share in the textbox below.

The CBA Section has a general comment about the lack of readability and length of the draft guidance. There is redundant text, and more plain language should be used.

The CBA Section is also concerned about the overall consultation process on an important OPC guidance. The OPC should have considered seeking feedback from relevant stakeholders on the existing biometrics guidance and reflect that feedback in draft guidance that would then be subject to a consultation process. Other process concerns include:

- **Online Questionnaire:** The questionnaire itself is too narrow in scope, and additional comments are limited by the text limitations in the questionnaire tool. A list of all the questions, as typically seen in consultations, was not made available.

- **Additional submissions:** The OPC indicated that it would not accept additional submissions beyond the online questionnaire. We find this surprising given the important issues raised by using biometrics and the need to ensure balanced guidance that addresses privacy considerations, legitimate business needs, individual expectations in an increasingly digital world, and legal certainty.

- **Roundtables:** The CBA Section is concerned about the lack of transparency regarding the roundtable process and questions the wisdom of not being more inclusive of all views from the beginning.

Finally, the CBA Section recommends that the definition of "biometrics" in the guidance be refined to consider the fact that not all information that is biometric in nature necessarily constitutes sensitive personal information, depending on the context. The risks posed by "biometrics" (as currently defined) to individual privacy rights depend on how organizations use or may use the information, rather than solely on its biometric nature. Adopting this approach would be in line with that taken by regulators under the EU's General Data Protection Regulation(GDPR).

The CBA Section is eager to work with OPC to share constructive feedback throughout the consultation process.

Best regards,

(original letter signed by Julie Terrien for Sinziana Gutiu)

Sinziana Gutiu
Chair, Privacy and Access Law Section