Response by the Centre for Information Policy Leadership to the Office of the Privacy Commissioner of Canada's Draft Guidance for Processing Biometrics – for Organizations

Submitted February 16, 2024

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the OPC's Draft Guidance for processing biometrics – for organizations (Guidance). CIPL recognizes that organizations need regulatory guidance clarifying their legal obligations when processing biometric data and greatly appreciates the Guidance and the opportunity to provide feedback. The field of biometric technology is growing quickly and facilitates a wide range of legitimate societal benefits, and, as such, is a primary research focus for CIPL.

CIPL will soon publish an in-depth report, entitled "Enabling Beneficial and Safe Uses of Biometric Technology through Risk-Based Regulations". In this report, CIPL details biometric technology use cases prevalent across sectors and the risks associated with said use cases. Use cases vary in risk and benefit, with some providing substantial benefits and low risks to individual rights, while others pose higher risks due to context, sensitivity, potential inaccuracies, biases, or lack of transparency and oversight. Importantly, CIPL details why the effective regulation of biometric systems requires a risk-based approach to avoid both over-regulating in cases of low-risk and under-regulating in cases of high risk and will share this report with the OPC as soon as it is published.

CIPL's feedback on the Guidance will focus on 1) scope and terminology, 2) consent, and 3) the application of a risk-based approach.

Scope and Terminology

While the PIPEDA does not mention biometric data or technology, OPC has stated that biometric data is generally considered sensitive under Canadian law. According to a May 2022 Interpretation Bulletin, "Biometric information is sensitive in almost all circumstances, as it is intrinsically, and in most instances permanently, linked to the individual." In the Guidance, the OPC broadly states that "biometrics are a category of sensitive data" and references "biometric information" and "biometric data".

To foster trust and responsible practices in the development and deployment of biometric systems, the Guidance needs to prioritize clarity and precision in definition, scope, and terminology. Significantly, the Guidance leaves terms like "biometric data" and "biometric information" undefined. The absence of definitions causes legal uncertainty and could lead to overly broad interpretations; for example, it is unclear whether photographs, video recordings, and audio recordings are considered biometric information or biometric data by the OPC.

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website (http://www.informationpolicycentre.com/). Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

CIPL recommends that regulations include heightened compliance requirements for specific types of biometric systems; they should target biometric systems that are intended to be used to identify individuals and exclude systems that are not intended to be used for identification purposes. To assess and establish the absence of an intent to use biometric systems for identification purposes the OPC should consider whether organizations that develop and deploy biometric technology take reasonable measures (e.g., technical, organizational, and contractual) to ensure that the processing of biometric data will not be used for identifying purposes. Laws and regulations should also explicitly exclude certain types of data (e.g., photographs, video footage, audio recordings) from the definition of biometric data.

Regarding terminology, many organizations that develop and deploy biometric systems incorporate vocabulary based on the International Organization for Standardization ISO/IEC 2382-37 (Third Edition, 2022-23) publication. ISO/IEC 2382-37 serves an important function because it establishes a consistent and systematic description of the concepts in the field of biometrics, which can promote interoperability across sectors and jurisdictions. In some cases, the Guidance diverges from emerging industry standards. For example, it discusses "authentication" in context of biometric technologies, but the use of "authentication" to describe biometric systems and capabilities is now discouraged according to ISO/IEC 2382-37. Such inconsistencies between regulatory guidance and standards can drive uncertainty within organizations that want to comply with OPC guidance.

Consent

The Guidance suggests that organizations "will almost always need to seek express consent" to process biometric data. However, the Guidance does not discuss under what circumstances express consent will not be necessary. CIPL welcomes more guidance from the OPC on this topic. Examples of when explicit consent will not be mandatory would help foster certainty.

Obtaining consent for processing biometric data can be impossible or inappropriate, especially in cases involving fraud prevention. Despite a rise in financial fraud incidents in Canada, many banks still rely on insecure SMS authentication PINs. In July 2022, Canada's Office of the Superintendent of Financial Institutions introduced Guideline B-13, requiring regulated financial institutions to implement risk-based identity and access controls, including multi-factor authentication (MFA) for cybersecurity. In online payments, behavioral biometrics, like keystroke analysis, device, and application data, create a unique profile for user verification. However, meeting MFA requirements often requires using behavioral biometrics without explicit customer consent, as seeking consent may compromise fraud prevention efforts.

The Application of a Risk-based Approach

A risk-based approach to biometric technology regulation enables tailored and contextual protections against the actual risks of specific use cases. Not all biometric systems should be considered high-risk. Indeed, in many instances, biometric systems can yield important societal benefits with low risk to individuals. Regulations must account for benefits and risks, without overregulating uses with minimal risks or underregulating uses with substantial risks.

The Guidance differentiates between mandatory measures ("You must") and recommended ones ("You should"). To enhance clarity on this distinction, CIPL recommends the OPC explicitly state that "should" signifies a recommendation, not an obligation, as clarified in PIPEDA.

The Guidance importantly acknowledges that "the implementation of technical … measures is an important factor in mitigating the privacy impacts" associated with the processing of biometric data. CIPL explores some such technical measures in a recent report, "Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age". As discussed on page 31 of that report, certain technical measures allow organizations to process biometric data in encrypted form on an end user's device (on-device processing). Organizations that deploy on-device processing can entirely avoid accessing an individual's biometric data and storing it on their own servers, which results in significantly lower risks to individuals. CIPL encourages the OPC to further explore the technical aspects associated with biometric technologies, including the use of PETs and PPTs to mitigate risks.