# Submission to the Office of the Privacy Commissioner by the Canadian Marketing Association on draft guidance for processing biometrics for organizations

February 2024

# Table of Contents

## Executive Summary

The Canadian Marketing Association (CMA) appreciates the opportunity to respond to the consultation by the Office of the Privacy Commissioner of Canada (OPC) on its draft guidance for processing biometrics. We appreciate the OPC's decision to extend the submission deadline and modify the submission format so that organizations could more fully participate in the development of guidance in this important area.

The responsible, secure use of biometric data provides many advantages for Canadian consumers and organizations, including enhanced security, accuracy, cost reduction, relevance and convenience.

Recent research has revealed that, as technology evolves, consumers demand much greater speed and quality of information so that they can readily access relevant products and services, benefit from offers and make informed purchase decisions. In the marketing sector, biometric data, used responsibly, can help marketers reach and serve consumers in the personalized and unique ways that they expect – including serving them with ads at ideal moments and in more meaningful ways.

We support the development of thoughtful regulatory guidance in this area so that consumers and companies can realize the advantages, while preventing the misuse of biometric data by unscrupulous players.

Privacy and technological innovation are not a zero-sum game. Both current privacy law (the Personal Information Protection and Electronics Document Act, or PIPEDA) and proposed privacy law (the Consumer Privacy Protection Act, or CPPA) recognize the dual purpose of protecting personal information and the needs of organizations to use personal information to innovate. Regulatory guidance must similarly forge a fertile environment for innovation while protecting Canadians' privacy rights.

Different levels of risk require different levels of regulatory emphasis that are proportionate to that risk. The draft guidance, as currently written, would be more reasonable for higher-risk biometrics and uses, rather than general guidance.

The OPC should adopt a more risk-based approach to this guidance. To ensure that biometric data is used responsibly for purposes that support consumers' interests and needs, the guidance must incorporate a spectrum of risk by:

- Including an element of unique identification into the definition of biometric data so that the definition is not unduly broad, and so that it aligns with the definition of biometrics in other jurisdictions, such as Quebec and the UK.
- Setting different standards for biometric data that is obtained for a temporary use (i.e., monitoring) versus data that is kept and re-used.
- Recognizing that biometric data, when de-identified and used only in a closed ecosystem, poses much less identifiability risk than it would, however small the risk might be, if it was used openly.

The guidance must also include a contextual approach to determining appropriate purposes by:

- Removing the over-emphasis on necessity in the guidance in favour of the more effective four-part test that has served organizations and consumers well through PIPEDA for more than two decades. This entails requiring organizations to assess sensitivity, effectiveness, proportionality, and necessity.
- Recognizing the reasonable and valid needs and wants of consumers who may consent to the use of biometrics to experience more convenience, and more tailored communications and advertising.

In general, the guidance should not go beyond what is required in the law, unless it is written as a best practice ("should") rather than a legal requirement ("must"). Several "must" statements in the draft need to be modified to reflect this principle.

The OPC guidance is set to be released while the Artificial Intelligence and Data Act (AIDA) is still being deliberated. There must be alignment between the OPC's guidance and any regulation of biometrics within AIDA if/when it comes into force.

# Key Recommendations

## 1. Incorporate a spectrum of risk

Like all personal information, biometrics must be considered along a spectrum of risk, with regulatory requirements varying according to context. This principles-based, technology neutral approach is a fundamental underpinning of PIPEDA that has helped to ensure that privacy law can respond to developments in technology without being unduly restrictive, so that personal information is protected while organizations and individuals can benefit appropriately from innovation. It is particularly appropriate in an emerging area where the potential uses and benefits of biometric technologies continue to evolve.

Considerations when determining the level of risk include whether the data identifies a unique individual (or is, for example, only used for categorization), the length of use of the data, and whether the information is de-identified and converted to a template so it can only be used in a closed ecosystem. The following sections elaborate on these points.

### *Identifiability*

The definition of biometrics in the proposed guidance is too broad, covers a wide range of biometrics with vastly different risks of identifiability, and equally diverse impacts on the privacy and security of Canadians, and treats all types of biometrics as high-risk.

Not all biometrics are used to identify or confirm the identity of an individual. The definition of biometrics in the guidance should be adjusted to incorporate the concept of unique identification. This would align the guidance with PIPEDA's longstanding and effective risk-based, proportionate and principled approach.

This will ensure the guidance is consistent with the approaches adopted in other jurisdictions, such as Quebec and the UK. Specifically:

- Guidance in Quebec defines biometric data as "systems used to identify or confirm the identity of individuals by using their biometric information, such as fingerprints, iris, or retina prints, hand and face geometry, or voiceprints." Emphasis is placed on the ability to *identify* individuals, so technologies that collect biometric data solely capable of categorization do not fall under the scope of the guidance and are less restricted in use.
- Guidance in the UK identifies two relevant categories: Biometric data and special category biometric data. Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data." Special category biometric data is defined as "biometric data used for the purpose of uniquely identifying (recognizing) someone." Under the UK's data protection law, only special category biometric data is subject to additional requirements and protections (such as privacy impact assessments, obtaining express consent, etc.).

### *Biometric categorization*

The guidance describes categories of biometrics without first adequately defining biometrics. Because of this, the categories can include things that are not necessarily biometrics. For example, device-based gestures such as keystroke patterns (as explained below), may be captured under the current definition. Yet, these typically do not provide sufficient information alone to identify an individual and are particularly

low risk when used for fraud detection/prevention. For example, keystroke patterns help organizations to identify if users are cutting and pasting information into fields, or if a human is entering information instead of a bot.

In the marketing sector, biometrics can be used for the purpose of categorization without creating a unique profile or identifying someone. For example, marketers can segment their audience based on their typing behaviour (i.e. keystroke patterns) and create personalized campaigns for each segment. This data can be used to tailor content and offers to the preferences and needs of specific groups of users, based on patterns found in their typing style and speed. Rather than identifying an individual, this data is used to categorize an individual for analytical and optimization purposes, without creating or storing any unique profiles of individuals. This poses a significantly lower privacy risk than biometrics (such as unique facial or fingerprint data) that can be readily used for identification purposes and would create potential for real risk of significant harm (RROSH) if breached.

Uniqueness and immutability should be included in the definition of biometrics so that the line is clearly defined.

***Temporary versus ongoing uses***

The guidance should set different standards for biometric data that is obtained for a temporary use versus data that is kept and re-used.

Monitoring biometric data means collecting and analyzing biometric data in real time, without saving or storing it for future use. This type of activity should be regulated to a lesser extent than data that is stored.

For example, some digital billboards capture and use facial data that registers reactions or emotions, or estimates age or gender so that a consumer can be shown an ad in the moment that is more likely to be relevant to them. The data is permanently deleted immediately after the ad is served. At no point does personal identification occur.

***Closed versus open systems***

The guidance should recognize that when de-identified biometric data is used only in a closed ecosystem, it does not pose the same identifiability risk as it would, however small the risk might be, if it was used openly.

For example, voice print data can help organizations confirm customers' identities and history with the company (including fraudulent activities) before presenting special offers and accommodations. If the data is de-identified to the point it is only useable in that closed ecosystem (and effectively useless elsewhere), retaining the data for the purposes of fraud reduction is a reasonable and legitimate use. Minimizing fraud is important for both consumers that are the victims and organizations that carry the associated costs, particularly small and medium-sized businesses, for which fraud can be particularly damaging and costly.

The guidance should recognize that data used within a closed ecosystem does not have the same level of sensitivity and should reflect current best practices for the treatment of de-identified information, along the lines of those put forward by the Canadian Anonymization Network (CANON).

## 2. Ensure a contextual approach to determining appropriate purposes

Organizations should carefully assess the appropriateness of purposes on a case-by-case basis, notwithstanding that biometrics are generally more sensitive than other types of data.

The most effective way to achieve this is to have organizations apply the four-part test used under PIPEDA to determine the appropriateness of purposes. This test requires organizations to equally assess sensitivity, effectiveness, proportionality, and necessity.

The guidance implies that if other alternatives exist, the use of biometrics is likely not permissible. There is a disproportionate focus on necessity, but necessity is just one part of the picture. There should be a focus on whether the purpose for the use of biometrics is legitimate. This aligns with section 12 (2) of the proposed CPPA, and with jurisprudence.

The guidance states that “if the underlying business or institutional rationale is to increase convenience or enhance customer experience, your biometric initiative is likely inappropriate.” This assumption should be removed as it ignores the reasonable and valid needs and wants of consumers who may opt-in to the use of biometrics in order to experience more convenience and ease-of-use, and more tailored communications and advertising. Recent research demonstrates that consumers desire convenience and relevant digital experiences and ads. More than 70% say they lose trust in a company when it sends them information about products and services that don't interest them.[1]

There are many instances where it is reasonable to allow biometrics to be used so that consumers receive the intuitive and personalized information and offers that they are increasingly demanding, as long as there is consent and appropriate safeguards in place.

From a consumer perspective, it should always be possible to consent to something you deem reasonable in the circumstance. For example, a consumer sitting in the back of a taxi should be able to provide their consent to engage with a digital billboard that takes cues from their facial expressions to provide them with more meaningful advertisements and local suggestions, after which the data is permanently deleted.

Similarly, it is not unreasonable for a consumer to provide consent to a wearable device/watch company for them to use biometric data (on their body movements) to deduce whether they may have an injury or impairment to suggest helpful products or programs.

In the case of market research, a consumer may agree, through opt-in consent, to engage with a wearable device that tracks general eye movements that provide insights into where the user’s eyes are most drawn to (in a physical space, or on a website). The data would be used for categorization purposes (i.e., not attributable to the individuals) to help companies make decisions about UX design, or to better serve people with compromised vision.

In all cases, the guidance should emphasize the four-part test mentioned above, rather than attempting to prohibit practices outright through “no-go-zones”. Broad prohibitions may stifle potential future innovation that would be beneficial for individuals.

## 3. General feedback

In general, the guidance should not go beyond what is required in the law, except when it is provided as a best practice (“should”) rather than a legal requirement (“must”). There are several “must” statements in the draft that need to be modified to reflect this principle, and to take into account the sensitivity of the information. Examples include:

- Consent: The guidance states that organizations "will almost always need to seek express consent". This should be replaced by "should always consider whether express consent is needed". This ensures a risk-based approach, and recognizes a spectrum of identifiability.
- Limiting Collection: When biometric characteristics are collected for the purposes of using them as a safeguard, the mandatory requirement within PIPEDA would be to ensure that the nature and sensitivity of (as opposed to the number**)** of biometric characteristics collected is appropriate. The guidance should allow for a similar risk-based approach. The requirement for organizations to limit the number of characteristics to the most appropriate level should be a “should” requirement and not a “must” requirement.
- Service Providers: The guidance propose that organizations name the service providers that they share biometric data with. This will make organizations more vulnerable to attacks from bad actors, allowing them to determine which control evasion is used by the relevant service provider.

[1] Consumer Privacy Research Findings, Sago, October 2023.

The guidance should only require organizations to share the categories of service providers with whom they share biometric data, wherever possible.

The OPC guidance is set to be released while AIDA is still being deliberated. There must be alignment between the OPC's guidance and any regulation of biometrics within AIDA if/when it comes into force.

## About the Canadian Marketing Association

The CMA is the voice of the marketing profession, representing corporate, not-for-profit, public, and post-secondary organizations across Canada. We help marketers and their organizations maintain high standards of conduct and transparency through our Canadian Marketing Code of Ethics & Standards, our extensive resources on privacy law and best practice, including a Guide on Transparency for Consumers, and our training and professional development programs, including our Privacy Essentials for Marketers course and the Chartered Marketer (CM) professional designation. Our Consumer Centre helps Canadians understand their privacy rights and obligations, and we respond to marketing-related enquiries from consumers and organizations.