Response to the OPC's Draft Guidance for Processing Biometrics – For Organizations
Friday, February 16th, 2024

Office of the Privacy Commissioner of Canada
30 Rue Victoria,
Gatineau, QC J8X 2A1
Canada

Email : OPC-CPVPconsult1@priv.gc.ca
CC: jbriggs@iabcanada.com, policy@iabcanada.com, IAB Canada Privacy Working Group Members

Office of the Privacy Commissioner of Canada,

IAB Canada on behalf of its members, would like to thank you for providing us with the opportunity to provide official commentary on the recently released draft guidance on the use of biometric technologies and an organization's responsibility when handling biometric information.

Established in 1997, IAB Canada is the only not-for-profit association exclusively dedicated to the development and promotion of the rapidly growing digital marketing and advertising sector in Canada. We were actively involved in discussions with your office in the past, and our members support your efforts to protect the privacy of Canadian citizens through the development of stronger guardrails around collecting and handling personal information.

Our estimated $16.8 billion Canadian digital advertising sector which employs over 50,000 Canadians, is committed to helping our government collectively work toward modernizing our digital capabilities to bring Canada to the forefront of responsible global digital innovation and economic growth. Protecting the data of Canadians is of paramount concern to our members and our industry is committed to supporting the efforts of your office as good privacy practices are ultimately good business practices.

It is our hope that this consultation will result in a balanced and fair set of guidance that will support both an organization's ability to responsibly use biometric data and consumer privacy protections while permitting Canadian businesses to compete in a rapidly evolving global market. We found the recent industry roundtable discussion on this guidance to be very insightful and we hope that you find our written recommendations and feedback to be useful as you work towards releasing what

will be final guidance. The growth and innovation in biometric technology is changing at a rapid pace and our members are using it in ways to increase the safety and protection of consumers as well as to improve the online consumer experience and we hope that you find our input to be valuable.

About IAB Canada:

IAB Canada represents over 250 of Canada's most well-known and respected stakeholders in the digital advertising and marketing sector, including advertisers, advertising agencies, media companies, digital media publishers and platforms, social media platforms, ad tech providers and platforms, data companies, mobile and video game marketers and developers, measurement companies, service providers, educational institutions, and government associations operating within the space. Our members include numerous small and medium sized enterprises.

Companies in the digital advertising and marketing sector offer a wide range of highly innovative products and services, including valuable service offerings to individual Canadians. This sector is intensely competitive, and the long-term success of our members is fundamentally predicated on their ability to continually design, develop, offer, and improve valuable digital products and services.

Our members include numerous small and medium sized enterprises and represent well over 80% of the estimated $16.8 billion industry in Canada. IAB Canada has a long history of creating programs designed to promote responsible growth in Canada's online advertising industry. IAB Canada is actively involved in productive policy discussions with various government departments including ISED, the OPC, the CAI, Elections Canada, AGCO and Health Canada.

Globally, the IAB network and our collective stakeholders have been committed to modernizing privacy compliance since 2016, having developed a proven privacy framework that ensures consumers are able to make choices online that are technically executed while providing the supply chain with an accountability stream which includes a record of consent status in compliance with cross-jurisdictional laws.

Developed by an international community comprised of the most respected technical engineers this global approach to responsible, privacy-protected media transactions was first-born in Europe in response to the GDPR. IAB Canada has recently released the framework in Canada to proactively help our market raise the bar on privacy technology for the purposes of online advertising.

The Transparency and Consent Framework Canada (TCF Canada) allows participants in the online advertising ecosystem to clearly and consistently communicate with Canadian citizens about how their data is being used, while also providing an opportunity for them to object and manage their consent preferences in accordance with jurisdictional privacy laws both federally and provincially. As new legislation comes to pass the Framework is updated accordingly.

Hundreds of Consent Management Platforms (CMPs) leverage this framework to provide content publishers with the peace of mind that their consent activity is being managed in a globally standardized way, eliminating risk for the industry and enhancing privacy protection for consumers.

Introduction

Our members use biometric technology in a myriad of ways to protect and improve their relationships with their consumers. Most of the use cases revolve around providing necessary security safeguards and combatting fraud. Some members use aggregated data to measure content engagement to better understand effectiveness of communications and to infer attitudes and preferences towards products and services. While it is used sparingly and with great caution, the responsible use of biometric technologies plays an important role in our industry.

IAB Canada's members understand the importance of the protection of privacy and data protection and appreciate the guidance coming from your office. While it is useful and provides some additional clarity around the specifics of the legal requirements, our constituents have some questions, concerns and areas requiring further clarification which we have outlined below.

1. **Not all uses of biometrics should be treated equally – need for individual assessments.**

The definition of biometrics included in the guidance is overly broad and will make compliance operationally difficult. We believe that the definition should be modified to allow for context to a specific purpose or use which we explain in more detail below.

The guidance states that biometrics are a category of sensitive information and that "you must obtain express, informed and specific consent when using biometrics" on the part of the individual. However, not all uses of biometric technologies collect data at the same level of sensitivity and carry the same risks. While consumer protection safeguards must be in place, they should be balanced with the necessary protection of an organization's ability to authenticate its users and to gain meaningful insights to improve the overall level of service.

In accordance with the guiding principles of PIPEDA, which dictate the requirement to balance the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information where businesses are required to engage in a "balancing of interests" between the individual and the organization concerned, we believe that this same principle should be applied to the use of biometric technology. Given the wide range of use cases for the use of biometrics (as broadly defined in the current guidance), our members feel it is appropriate to conduct thorough assessments *prior* to implementing the use of the technology. This would allow organizations to determine appropriate and proportionate notice, consent, collection, and safeguarding practices based on a well-defined evaluation against the sensitivity, necessity, effectiveness, proportionality, and minimal intrusiveness criteria as laid out by the OPC.

The guidance defines biometrics as "the quantification of human characteristics into measurable terms. They are used for recognition and, less commonly for categorization." The guidance goes on the outline the stages of how biometrics are being used and outlines them as Enrollment, Storage and Matching.

Most stakeholders in the digital advertising industry use biometrics for the purpose of gaining valuable market insights in an aggregated, non-identifiable way to provide an enhanced level of service to their customers. This use case provides Canadian businesses with reliable and privacy-protected data to innovate and better develop their offerings to compete on a global stage. There are instances where a product or service would be degraded in the absence of biometric data and therefore would necessitate consent as a condition of the product or service delivered. The current guidance does not include this use case in its definition and should be revised accordingly.

To further demonstrate this use case, consider the efforts made to provide accessibility of content and information. As consumers embrace advanced technologies that facilitate hands-free vocal interaction, the use of spoken prompts will play a critical role in communications generally. The use of voice recognition will help facilitate the types of content and ads that are most appropriate according to characteristics as fundamental as language. This use case works in direct alignment with serving Canada's diverse multi-cultural population and plays an important role not only to deliver accessibility but also to stay in compliance with French language legislation.

Biometrics in marketing helps Canadian businesses reach the right audiences using science. Reducing identifiable factors that enable the aggregation of biometric data sets may provide meaningful innovations that can provide probabilistic classification of important audience attributes like age range to further protect from unintended exposure to regulated categories.

With appropriate guardrails, biometrics can be used to help businesses build better experiences for consumers. De-identified and aggregated eye movement and scrolling tracking can help content publishers understand which content is of most interest. For example, a retailer's website would allow for enhanced design for user experiences or to provide research data about what products consumers spend the most time with to help guide future product development. With adequate transparency and notice and an option to opt-out, this type of use case should be exempt from requiring express consent.

Another critical and essential use of biometric technologies deployed by some of our stakeholders is directed toward the fight against identity fraud. The use of behavioural biometrics such as keystroke patterns to identify unusual behaviour could help trigger a secondary factor of user or subscriber verification. This is another case where the data being collected is less sensitive. In the absence of collecting personally identifiable data in this case, an appropriate assessment prior to deployment would conclude that it is exempt from the express consent requirement. The current guidance needs to be amended to allow for these case-by-case assessments using the tools afforded to us in PIPEDA.

We would recommend that the guidance be edited to acknowledge that not all biometrics are necessarily sensitive information.

2. **Concerns around third party accountability and transparency requirements**

Most organizations using biometric technologies rely on third-party service providers and do not build the systems themselves. In some cases, the collection of biometrics is implemented by a third party completely independent of the organization. This scenario is commonly seen in an app

environment where the browser uses a biometric such as a fingerprint or facial recognition as a frictionless verification factor to permit access to an organization's product or service.

As within any third-party relationship, partners are carefully selected with detailed agreements outlining the specific contractual obligations including those specific to the collection, safeguarding and transferring of any potentially sensitive consumer information.

While it is crucial that any guidance specific to biometrics addresses the use of third parties, IAB Canada believes that the requirement that an organization "must ensure your collection from third parties is lawful" goes beyond existing and other jurisdictional requirements. We believe that an organization should not be held entirely accountable for the actions of their partners, but they should be obligated to "ensure proper grounding in law at every step of the data flow for which they are involved" and are able to rely on signed contracts for assurance of best practices.

Large-scale organizations work with numerous partners who change on a regular basis. The current guidance outlines an obligation that an organization must list and make available the names of the individual partners they work with to consumers. Going well beyond both the global standard and more locally, higher than the expectations of Quebec's Law 25, this is an overly burdensome requirement providing minimal value to an individual. The value to consumers lies in the types of providers their information is being shared with as opposed to the actual names of the providers themselves. Therefore, listing categories of third parties is a more realistic and meaningful expectation and we would like to see this modified in the guidance.

3. Avoid the use of "Must" and "Should"

Throughout the document the guidance is framed by telling organizations what they "must" and "should" do when working with or using biometrics. While we appreciate through our discussions with your office, that this was meant to be helpful, it does lead to some confusion and implies that any advice coupled with a "must" is legally binding vs. a strong recommendation or best practice. Organizations should be expected to assess their practices against the statute, conduct the necessary internal assessments and make decisions on how to apply the guidance to protect their consumers when using biometrics.

IAB Canada recommends that the wording be amended to limit confusion and that the OPC considers including more examples of best practices or of appropriate uses against each of the criteria.

4. **Misalignment with other requirements – questions around interoperability**

There are several other areas within this guidance that could be more closely aligned with global standards and/or existing legislation. These areas include:

Definition of Biometrics

As mentioned earlier in the document the current definition is too broad and should be rewritten to allow for context to a specific purpose or use. This would make compliance more straightforward and align with practices in other markets/standards. Further, we believe that replacing the term "biometrics" with the term "biometric data" would bring the guidance more closely in alignment with the GDPR and would reduce confusion in the sector.

Safeguard Requirements

The guidance states that "Biometric data **must** be stringently protected with a **higher** level of security safeguards". This requirement should be changed to a "high" level as it could be deemed appropriate to protect biometric data at the same level as other types of sensitive information (i.e. Credit card information) and higher implies always more which may not be realistic.

Breach Reporting

The breach reporting requirements outlined in the document are concerning as they overwrite the law and should be modified to meet the standard set out in PIPEDA. Our federal privacy law allows for a case-by-case assessment of the potential risk of significant harm resulting from a data breach nor does it account for the breach of any biometric data that is encrypted in a form deeming it inaccessible.

Retention and Deletion Procedures

The retention and deletion policies should follow what is laid out in applicable laws. Under PIPEDA biometric data should be deleted as soon as its purpose has been fulfilled unless its retention is required by law.

5. Why now? Let's wait for C-27.

While we appreciate the need to continue moving forward on revising outdated guidance to match with the changing environment, we do have concerns with it being so closely dependent and integrated (and in some cases more burdensome) with PIPEDA when we are so close to federal privacy reform. While the Committee of Industry and Technology is in the final stages of passing Bill C-27 – a bill that would fundamentally change the rules of engagement for business – we suggest that you wait and revise the guidance to match new provisions should the bill pass. The CPPA has much higher requirements in the areas of notice and consent with direct implications on the use of biometrics and with organizations already managing some significant operational compliance changes, hitting pause would alleviate the pressure on operational and financial resources.

However, should you continue to move forward, it would be helpful if in the guidance you could specifically address what the status of the guidance will be once C-27 becomes law and whether it will remain in effect beyond PIPEDA.

In Closing

Thank you considering IAB Canada's thoughts on the recent draft guidance on privacy and the use of biometric technologies. Biometrics in the digital advertising sector is used with great caution and specific purposes that contribute to consumer safety while enabling Canadian businesses to compete on a global stage. We hope this feedback is helpful to your office as you contemplate this important technology.

IAB Canada encourages you to reach out to us at any time with any questions or feedback regarding this submission, and we look forward to participating in upcoming consultations and discussions to further address the specifics of the guidance and the impact on the digital ecosystem.

Sincerely,

Sonia Carreno
President, IAB Canada,
scarreno@iabcanada.com