12 January 2024

Hon. Philippe Dufresne
Commissioner
Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

RE: Comments of ACT | The App Association, *Draft guidance for processing biometrics*

ACT | The App Association hereby submits comments on the Office of the Privacy Commissioner of Canada's (OPC's) new draft guidances on biometric technologies for organizations and public institutions.[1]

The App Association represents thousands of small business application developers and connected device companies, located both within Canada and across the globe. These companies drive a global app economy worth more than CAD $2.1 trillion, and this economy continues to grow.[2] App Association members leverage the connectivity of smart devices and the patient-generated biometric data they generate to create innovative solutions that introduce new efficiencies across consumer and enterprise use cases; therefore, OPC's effort to develop guidance on privacy obligations, considerations, and best practices for handling biometric information is directly relevant to us, and we urge for the careful consideration of our views.

App Association small businesses (and others) who rely on innovative digital products and services expect their valuable data is kept safe and secure, particularly their sensitive biometric data. The community the App Association represents practices and promotes responsible and efficient data stewardship to solve problems identified across consumer and enterprise use cases. Consumers, as well as stakeholders throughout the value chain, have strong data security and privacy expectations, and, as such, ensuring that the data collection and use practices reflect those expectations by utilising the most advanced technical protection mechanisms (*e.g.*, end-to-end encryption) is a market-driven necessity. The App Association recognizes that privacy and security are a shared responsibility, and we serve as a leading resource in the biometrics and privacy space for thought leadership and education.

Initially, the App Association notes its agreement with OPC's statement the biometric data is a key means used "to facilitate more efficient access to goods and services while adapting to evolving security risks," which reflects that biometric data's use is integral to the future of Canadian consumer and enterprise markets. For example, the demonstrated benefits of collecting and timely acting on patient-generated health data include reduced hospitalizations

[1] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-bio/.

[2] See https://actonline.org/global-appcon22-competition-and-privacy/.

and cost, avoidance of complications, and improved care and satisfaction, particularly for the chronically ill. The App Association urges OPC to ensure that its guidelines advance a seamless and interoperable digital economy that leverages the power of biometric data because Canadian consumers now expect access to seamless and secure data across the services they use. Further, the responsible collection and use of biometric data should contribute to the investment in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining artificial intelligence (AI) systems, ultimately offering a pathway for the voluntary adoption and integration of those AI systems.[3]

Generally, the App Association urges OPC to, consistent with the Personal Information Protection and Electronic Documents Act (PIPEDA), ensure that its guidances on biometric technologies leverage an approach based on established risks and harms (not edge/rare use cases or hypotheticals), that recommended measures to manage risks are scaled to the harms presented, and that those who know or should know about a risk and have the ability to take action to mitigate that risk have the appropriate incentives to do so. Such an approach is consistent with leading standardized practices for supporting information security, cybersecurity and privacy protection.[4] Across its suggested requirements ("You Must") and recommendations ("You Should"), we request that OPC provide clear language to clarify that steps taken to mitigate harms may change in severity depending on the risk presented by the data collected and use(s) of it. Without this important concept's reinforcement across its guidances, organizations and public institutions will, in the spirit of compliance, be forced to apply the same risk management approach to all uses of biometric technologies regardless of the risk posed.

We applaud OPC's alignment in both draft guidances with key concepts such as data minimization, informed consent to data use and adherence to promised uses of data, reasonable reporting and disclosures per PIPEDA, product lifecycle risk management, and the assignment of responsibility based on knowledge and the ability to take action to mitigate identified risks. These practices, used at scale to the risk posed by the specific fact pattern, are endorsed and promoted by the App Association, and are widely practiced by App Association who have long recognized that responsible data stewardship is a key differentiator in the marketplace.

Based on the App Association's members experiences in leveraging numerous innovative biometric-assisted technologies in order to provide services consumers need and demand in the digital economy, we elaborate on two key uses cases: facial verification and wearable devices:

Facial Verification

Facial verification technologies are most often used for security purposes, i.e., to verify whether a person really is who they say they are. For example, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log in to apps using a scan of their face from the camera app. An

[3] We encourage OPC and other Canadian policymakers to align with the App Association's responsible AI policy recommendations, available at https://actonline.org/2023/07/10/act-provides-policy-recommendations-for-ai/.

[4] https://www.iso.org/standard/71675.html.

app developer can choose to integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.[5]

As the underlying technology continues to improve, app developers are likely to implement a greater variety of facial recognition use cases. Therefore, it will become increasingly important that emerging standards of regulation ensure that appropriate governance and accountability structures attach to each use case commensurate with its risk. For example, in existing risk frameworks created by academics, targeted use of facial verification algorithms on a one-to-one basis typically represents a lower risk deployment, whereas real-time deployment of facial identification in public spaces is among the highest.[6]

The App Association notes its support for policies that would scale up requirements for particularly risky uses of facial recognition technology and that would limit how companies can process consumer data without their consent.[7] To the extent possible, OPC should differentiate between targeted, consent-based uses of biometrics versus drag-net applications will be an important task going forward.

Wearables

Through the App Association's Connected Health Initiative (CHI),[8] the App Association seeks to advance responsible pro-digital health policies and laws that can harness the great potential of connected healthcare devices and tools, some of which may leverage biometric inputs, to unlock a higher standard of care for patients while minimizing potential harms. The remote collection of health data through wearables can help ameliorate some of the long-standing disparities in healthcare access by allowing personalized diagnostics to occur outside of traditional healthcare institutions. For example, fitness trackers that collect valuable data, such as sleep patterns, activity, and stress levels, can automatically share relevant information with clinicians, therapists, or coaches so that they can use granularized data to create more personalized care routines without requiring an in-person visit. Recently, many consumers have turned to

[5] Apple, "About Face ID advanced technology," September 14, 2021, https://support.apple.com/en-us/HT208108

[6] Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Risk Framework," Georgetown Center Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/risk-framework

[7] ACT | The App Association, "Testimony of Morgan Reed, President at ACT | The App Association Before the U.S. Senate Committee on Commerce, Science, and Transportation on Protecting Consumer Privacy," September 19, 2021, https://actonline.org/wp-content/uploads/Reed-Testimony.pdf

[8] www.connectedhi.org.

digital health platforms, tools, and services to consult with caregivers in greater numbers, and wearable ownership and use continues to increase year over year.

Clearly, usership of technologies that can pull biometrics and infer cognitive or emotional states will continue to increase, especially as efficacy improves and the benefits become clearer to users. The App Association is keenly aware of the need to create appropriate guardrails to keep up with the growth of these practices and to ensure that mobile health players that collect sensitive biometric data continue to do so responsibly. The App Association continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of emerging technologies, such AI innovations.[9]

In conclusion, the App Association strongly supports risk-based guardrails around the use of biometrics that provide the public with a baseline level of trust and that set a clear set of expectations for the businesses that seek to do good through these services. We thank OPC in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

[9] E.g., https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf.