September 10, 2024

Philippe Dufresne
Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

Re: **Comments of ACT | The App Association re: the Office of the Privacy Commissioner's Exploratory Consultation on Privacy and Age Assurance**

ACT | The App Association (App Association) respectfully submits its views to the Office of the Privacy Commissioner of Canada (OPC) on its request for public comment on its exploratory consultation on privacy and age assurance.[1]

I. Introduction and Statement of Interest

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. The value of the ecosystem the App Association represents—which we call the app economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2]

Trustworthiness and safety are integral for the success of innovators in the mobile app economy, especially for smaller tech companies that may not have substantial name recognition. The prioritization of strong health, safety, and privacy protections is even more important for vulnerable populations like children, serving as a key component to developing consumer trust in the tech-driven products and services our members provide. The App Association helps shape and promote privacy best practices in a variety of contexts, including for apps directed to children and digital health tools, making us well positioned to provide insight to OPC.

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

[2] ACT | The App Association, State of the App Economy (2022), https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf

For example, the App Association has played an active role to make sure that the small business community is aware of their responsibilities under the Children's Online Privacy Protection Act (COPPA) Rule administered by the United States Federal Trade Commission (FTC). The App Association created a checklist for apps that are made for children to ensure that there is a free accessible resource for small businesses to use as a guide to comply with the COPPA Rule.[3]

While the App Association supports protecting children's privacy, over time rules in a number of jurisdictions have disproportionally squeezed small developers out of the market for apps and software programs directed at children. We encourage the OPC to consider the challenges small businesses have faced under other legal frameworks when considering new requirements. Such requirements should be reasonable and effective so that small developers can become compliant while still providing new and novel technology for the next generation.

II. The Current State of Children's Online Usage and Parent Engagement

According to the App Association's research, 85 percent of parents have concerns about their children's digital privacy.[4] PricewaterhouseCoopers (PwC) says that kids aged 8 to 18 spend an average of 7.5 hours in front of a screen for entertainment each day.[5] With this high amount of screen time for children, in combination with the high percentage of parental concerns held with respect to their children's privacy, one would assume that parents would actively take steps to address their children's screen time, such as enabling parental control settings on their children's' devices to make sure they do not have access to inappropriate information and reading privacy policies that the child may not understand due to their age and lack of life experience. Yet, research shows that only half – and, depending on the specific modality, less – limit screen time or use parental settings on their children's device.[6]

The research demonstrates that while parents often say they care deeply about their children's privacy, their actions display less concern. Parents may also feel that they should not be the ones responsible for setting the parental controls in place. Indeed, many parents would prefer that app developers provide free educational applications that help their child learn how to read, understand their multiplication tables, or provide some entertainment with the needed privacy provisions already in place to protect their children. However, developers with children-directed apps must balance using financial resources to stand out in a competitive app market with the costs of complying with

[3] https://actonline.org/family-app-privacy/

[4] Morgan Reed, *Developers and COPPA: Their Real-World Experience*, F.T.C. COPPA WORKSHOP, https://www.ftc.gov/system/files/documents/public_events/1535372/slides-coppa-workshop-10-7-19.pdf (October 7, 2019).

[5] https://www.cdc.gov/nccdphp/dnpao/multimedia/infographics/getmoving.html.

[6] https://www.statista.com/statistics/232345/parental-control-over-childrens-media-consumption-in-the-us/.

general privacy laws and other children's privacy laws and regulations. We urge OPC to help minimize these burdens to promote innovation.

III. The App Association's Views Regarding Mechanisms for Obtaining Age Assurance

Any requirements for obtaining age assurance of particular users should consider the practical compliance challenges that arise from the fact that many apps integrate into and operate through mobile communications platforms maintained by a different operator. As a result, certain information—such as the user's IP address, device ID, username, or screen name—sometimes shares automatically between the app developer and the platform provider when a user runs the application. This limited information sharing supports (and is often necessary for) the technical and operational functioning of the app. Therefore, we support OPC's position that requirements should be proportionate to the risk involved in different types of data collection and sharing. The level of risk of a back-end service provider obtaining a young user's screen name in order for an app to function should likely not pull otherwise unaware providers into a strict age verification compliance regime.

Indeed, age verification requirements that are too strict run the risk of incentivizing broader and more invasive data collection on young people. Regulations that do not take risk-based context into account may end up requiring entities who would not otherwise be aware of any sensitive information of minor users to go to great lengths to confirm whether their users are minors through continuous data collection and monitoring. Such an approach not only risks undermining broader privacy rights but also directly conflicts with the advocacy of the App Association and others for national jurisdictions to develop reasonable data minimization frameworks to enhance the privacy and security of people of all ages. Forcing platforms to collect more personal information about children could lead to severe privacy breaches and misuse of sensitive data, making kids more vulnerable instead of safer.

The App Association also urges OPC to refrain from supporting age assurance requirements that are too prescriptive with regard to the technical means such assurance is to be carried out. Due to the interconnected and constantly evolving nature of the app ecosystem, specific steps set in stone today for developers to follow may be out of step with technology in relatively short order.

The App Association notes that some platforms already implement procedures for obtaining age assurance and parental consent by offering family plans to sign up and use a platform along with providing parents optional settings for their children such as "asking to buy," rejecting or approving a purchase, monitoring content, or placing limits on screen time from the parent's device. This allows a parent a simplified process to see what their kids are doing on their devices and decide what limits they want to set for their children, and ensures that parents have meaningful notice of and control over how an app collects, uses, and discloses their children's personal information without imposing unnecessary burdens and costs on app developers.

The App Association therefore supports proposals to widen the range of approved methods for obtaining age assurance that may be used at the option of the operator, including text messages, knowledge-based authentication, and facial recognition technology. Already used for two-factor authentication across a range of contexts, some of these options are widely used modalities that can and should be relied upon.

In addition, we encourage OPC to ensure that new rules do not introduce unneeded friction into the process of parents allowing their children to sign up for and use apps. For example, the App Association supports rules in other jurisdictions such as the United States FTC's COPPA rule allowing operators to gain consent for third-party disclosures as part of the broader first-party process for consenting to the underlying collection/use of personal information (e.g., a disclosure and checkbox). Further, once a parent has provided consent to a third party to make disclosures through parental controls settings, this choice need not be reaffirmed separately in the process of obtaining parental consent.

IV. Conclusion

We thank OPC for the opportunity to comment and hope the information we provided helps further the development of age assurance frameworks that balance innovation with the need to protect children's privacy and online safety.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

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