

Feedback on the Office of the Privacy Commissioner of Canada's Exploratory consultation on privacy and age assurance

Submitted by: Riley McNair, MSc, Faculty of Information, University of Toronto
Sara M. Grimes, PhD, Faculty of Arts, McGill University¹
September 10, 2024

We welcome the opportunity to submit the following in response to the Office of the Privacy Commissioner of Canada's (OPC) request for feedback regarding its plans to undertake policy and guidance work on the development and use of age-assurance technologies. We are academics from the University of Toronto and McGill University, with expertise in the areas of children's digital technology use and regulation, conducting research on the impacts of digital platforms on children's privacy and other rights. We are currently collaborating on a multi-year investigation² of the reach and impact of the Age Appropriate Design (AAD) Code (the Children's Code), a set of standards launched by the UK Information Commissioner's Office (ICO) in 2021 to advance children's privacy rights and best interests across the digital environment.³ AAD has since become the basis of a growing number of child privacy- and safety-by-design policies in Europe, Asia, and parts of the US, and has had a measurable impact on tech industries worldwide. We are contributing to this call for feedback because age-assurance technologies are a focus of our collaborative and respective research and have important implications for children's privacy, access to information, and other cultural rights.

We have answered all four of the questions listed in the call for feedback. Our full responses provide context and rationale to the positions for which we advocate, grounded in previous relevant research and scholarship. Our responses are furthermore informed by our own research and in-depth knowledge of current and emerging trends in comparable regulation and regulatory debates in the UK, EU and US; of dominant trends in the tech industry's past and recent responses to child safety and children's privacy; as well as our recent project findings on Canadian children's own experiences and thoughts about age appropriateness, age bans, and privacy in the digital environment.⁴ We have also included a summary of the six main recommendations proposed in our responses, which you can find on page 9 of this document.

¹ Please send correspondence to Professor Sara M. Grimes, sara.grimes@mcgill.ca.

² The Children and Age-Appropriate Game Design project is funded by the Social Sciences and Humanities Research Council of Canada (SSHRC).

³ "Age appropriate design: a code of practice for online services," Information Commissioner's Office, 2024. [LINK](#)

⁴ Swerdfager, B., Grimes, S. M., McNair, R., & Bui, A. (2024). *Child Appropriate Game Design Project Report: Year One*. [LINK](#)

1. What additional context should we be aware of in developing our future work?

Age-assurance technologies are often described by the companies that develop them as useful tools for the provision of “age-appropriate” online experiences for children.⁵ When evaluating the efficacy and appropriate use of age-assurance systems, it is useful to first consider the meaning of age appropriateness and its role in improving children’s safety and wellbeing in a digital world. Research has shown that age appropriateness is socially constructed; culture and demographics influence interpretations and experiences of age appropriateness across populations.⁶ Our own research with children shows that children and parents/caregivers largely determine age appropriateness on a case-by-case basis, based on each individual child’s developmental capabilities, maturity, digital literacy, and personal preferences. Recent research commissioned by the ICO and Ofcom found that many parents believe that age restrictions on social media or online games are arbitrary and an unreliable indicator of what is appropriate for their child.⁷ The UN Committee on the Rights of the Child confirms that age alone does not determine the types of risks and opportunities children encounter in the digital environment, highlighting that children’s, skills and stage of development are also key factors.⁸

Designing online environments in children’s *best interests* does not mean treating all children the same. Acknowledging the developmental and individual differences among children is fundamental to a ‘best interests’ approach to the design and regulation of online technologies,⁹ as established in the United Nations Convention on the Rights of the Child (UNCRC) General Comment No. 25 (GC25) on children’s rights in the digital environment. While the GC25 offers useful guidance on applying the best interests principle in practice, it remains a challenge for policymakers and technology companies to know how to adequately recognize children’s rights and evolving capacities instead of combatting online risk by broadly restricting or limiting their access to digital spaces.¹⁰ With a focus on age (or approximate age) as the determining factor in restricting or granting access, age-assurance systems do not in themselves afford a consideration of children’s best interests. They instead implement and enforce decisions about age appropriateness, some of which are based in law or scientific evidence, but most of which are not. The lack of transparency or dialogue around most of the decisions made about age appropriateness is a key concern.

⁵ “Internet Day 2024: Creating age-appropriate experiences with Kids Web Services,” Yoti, February 6, 2024. [LINK](#)

⁶ Bui, A., Grimes, S., & Brown, D. (2022). *The Media Ratings Project Report: A Cross-Cultural and Cross-Media Comparative Analysis*. KMDI. [LINK](#); Corsaro, W. A. (2005). *The sociology of childhood, 2nd ed* (pp. xiv, 359).

⁷ ICO and Ofcom. (2022). *Families’ attitudes towards age assurance: Research commissioned by the ICO and Ofcom*. GOV.UK. [LINK](#)

⁸ UN Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children’s rights in relation to the digital environment*. [LINK](#)

⁹ Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children’s understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society, 24*(4), 557–575. [LINK](#)

¹⁰ Livingstone, S., Third, A., & Lansdown, G. (2024). Children vs adults: negotiating UNCRC General comment No. 25 on children’s rights in the digital environment. Chpt. 31 in Puppis Et Al. (Eds). *Handbook of Media and Communication Governance*. Elgar Online; Khazova, O. (2021). How to ensure wider implementation of the CRC. In *Global Reflections on Children’s Rights and the Law*. Routledge.

The ICO's position on age assurance draws directly from the UNCRC and provides information on how children's right to privacy protections, access to leisure, play and culture, and protection from sexual exploitation can be preserved in age-assurance systems.¹¹ The ICO's position on age assurance emphasizes that respect for the views of the child need to be considered in age assurance processes. This is of the utmost importance because "children's participation rights are fundamental to the exercise of all their other rights."¹² Indeed, guidance on the development and implementation of age-assurance systems in Canada should first and foremost be informed by research that consults children directly about their needs, concerns, and desires for safer digital spaces. We recommend that the OPC consider commissioning research with children of diverse ages to get a better sense of their opinions and experiences of these systems.

2. Are there other privacy considerations we should we aware of?

The identification of citizens during age assurance processes online can have adverse consequences for their right to privacy and to their wellbeing. When individuals' identities are connected to their online activities, highly sensitive information about their personal characteristics, health, finances, and political beliefs may be accessed by government and corporate entities¹³ for policing, political profiling, or targeted advertising.¹⁴ This can result in a loss of anonymity that discourages people from operating freely in the digital environment¹⁵ and discriminatory profiling and advertising practices that target or exclude users from encountering important information about employment, healthcare, housing, and other essential services based on their ethnicity, religion, or sexual orientation.¹⁶ When leaked, users' personal data may be obtained by malicious actors for the purposes of identity theft or extortion.¹⁷ The OPC's preliminary privacy analysis includes identifiability as a high-level impact of age assurance; however, it does not distinguish the heightened risks posed by identification during biometric age assurance processes.

¹¹ "Age assurance: estimating or verifying the age of service users," Information Commissioner's Office, 2024, [LINK](#)

¹² Livingstone et al., 2024

¹³ Hinds, J., & Joinson, A. N. (2018). What demographic attributes do our digital footprints reveal? A systematic review. *PLOS ONE*, 13(11), e0207112. [LINK](#)

¹⁴ Shapiro, A. (2017). Reform predictive policing. *Nature*, 541(7638), 458–460. [LINK](#); Matz et al. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, 114(48), 12714–12719. [LINK](#)

¹⁵ Sas & Mühlberg. (2024). *Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective*. [LINK](#)

¹⁶ Speicher, T., Ali, M., Venkatadri, G., Ribeiro, F. N., Arvanitakis, G., Benevenuto, F., Gummadi, K. P., Loiseau, P., & Mislove, A. (2018). Potential for Discrimination in Online Targeted Advertising. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 5–19. [LINK](#); Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes. *Proceedings of the ACM on Human Computer Interaction*, 3(CSCW), 199:1-199:30. [LINK](#)

¹⁷ Sas & Mühlberg, 2024

Special provisions for processing biometric data during age assurance processes should be introduced because biometric data are unique, unalterable, and comprehensive. Unlike other personal information that can be changed, updated, or ‘forgotten’, biometric data such as fingerprints or facial data cannot be modified once collected, significantly impacting citizens’ right to privacy if these data are compromised. Notably, biometric age-assurance technologies, such as facial age estimation, are often marketed as “privacy-preserving” by their developers because they do not “cross-check people against a big database of faces” like facial recognition technologies do, nor do they require people to provide banking details, government identification, or other forms of “personal information.”¹⁸ This description of facial analysis for age assurance rests on an assumption that needs to be interrogated: biometric data are not personal information, and identification is the only harm arising from the collection of biometric data.

Identification is not the only potential harm arising from the implementation of age-assurance systems online. As outlined in the OPC’s preliminary privacy analysis, risks can also emanate from metadata retained by age-assurance systems and the normalization of age verification processes in the digital realm. Another potential harm could arise from the use of data collected during age assurance processes for the creation or optimization of artificial intelligence (AI) tools. In data capitalism – the economic logic underpinning the tech industry’s practices – data do not need to be collected for the purposes of identification to be valuable. Data are a financial resource that companies can leverage to drive profit through targeted advertising, personalized services, and the development of new technologies. Behavioural and biometric data are also collected and used by companies for more overtly problematic forms of commercial surveillance and exploitation, as is the case with “dark patterns”¹⁹ and certain forms of “emotional AI”.²⁰ In this system, any data collected can and will eventually be made useful even if it is not immediately commodifiable.²¹ Indeed, “much data gathered by corporations may lack a value until a specific use for it can be found in the context of much larger data sets.”²²

Data collected for age assurance processes might not be used to identify citizens, exposing them to profiling or identity theft, but they are susceptible to being used by governments and/or private companies to model trends about populations and optimize new technologies.²³ Importantly, these data could be used to train AI decision-making systems that influence citizens’ experiences in online and offline realms. When demographic or behavioural data are

¹⁸ “Everything you need to know about our facial age estimation technology,” Yoti, 2022. [LINK](#)

¹⁹ Beauvais, M., Grimes, S.M., Jayemanne, D., Giddings, S. (2022). Children’s Privacy and Video Games: Comments on Commercial Surveillance. Response to the US Federal Trade Commission’s advance notice of proposed rulemaking on commercial surveillance and data security (ANPR R111004) (Washington, DC). [LINK](#)

²⁰ McStay, A., & Rosner, G. (2021). Emotional artificial intelligence in children’s toys and devices: Ethics, governance and practical remedies. *Big Data & Society* (Jan-June), 1-16.

²¹ West, S. M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 58(1), 20–41. [LINK](#); Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

²² Couldry & Mejias, 2019

²³ West, 2017

used to power AI systems that predict or manipulate people’s outcomes, individuals lose autonomy. Research has shown that citizens’ personal data have already been used in this way by: Child Protection Services to create predictive risk models that determine which families require intervention;²⁴ police forces to build intelligence tools that identify potential crimes and the people who might commit them;²⁵ and the credit-scoring industry to develop big-data scoring tools that incorporate peoples’ personal characteristics and online behaviours into credit decisions.²⁶

Not only are these tools predisposed to exacerbating racial, gender, and socioeconomic biases and discrimination, but they can also “become co-creators and shapers of the environments they analyze.”²⁷ If stored, analyzed, or shared beyond their original purpose, data collected through age-assurance systems are at risk of being used in the development of AI decision-making tools that shape people’s access to social services, financial opportunities, and interactions with the criminal justice system. This poses a threat to citizens’ right to self-determination, which is integral to privacy because it ensures individuals have the autonomy to control their personal information and make informed choices without external interference.

3. Do you have any comments on our preliminary views?

The implementation of age-assurance systems online should be appropriate to the relevant risks of collecting, processing, and storing citizens’ data. This is reflected in the OPC’s preliminary position and is articulated in both the Children’s Code (mentioned above) and the California Age Appropriate Design Code Act (CAADCA) as a ‘risk-based approach’ to age assurance, which entails establishing the age range of users with a level of certainty that is appropriate to the risks, rights, and freedoms that arise from the associated data processing.²⁸ Age assurance impacts everyone, not just young users. Age-assurance systems, especially those that rely on biometric technologies, increase both the size and complexity of data processing on citizens. The widespread implementation of these systems online could increase risks of harm from profiling, identity theft, and data fraud. In addition, these processes enhance opportunities for government and corporate interference in citizens online and offline activities, which may degrade their autonomy, ultimately threatening their rights to privacy and self-determination as ratified in the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights. To mitigate these risks, the introduction of age-assurance systems, especially those that process biometric data, should be strategic, proportional, and on a needs-must basis.

²⁴ Centre for Public Impact. (2018). *Allegheny Family Screening Tool: A Case Study on the Use of AI in Gov...* [LINK](#)

²⁵ “Gangs violence matrix,” Metropolitan Police, 2024. [LINK](#)

²⁶ Hurley, M., & Adebayo, J. (2016). Credit Scoring in the Era of Big Data. *Yale Journal of Law and Technology*, 18, 148–216.

²⁷ Redden, J. (2020). Predictive Analytics and Child Welfare: Toward Data Justice. *Canadian Journal of Communication*, 45(1), 101–111. [LINK](#)

²⁸ “Age assurance for the Children’s code,” Information Commissioner’s Office, 2024. [LINK](#)

Age assurance should not be relied on as a first-line strategy for implementing online safety regulation. There is increasing recognition that children should be protected from harm online, and the rapid introduction of new online safety legislation across North America, Europe, and other parts of the world reflects this. Some of these legislative developments, such as new state-level laws in Texas (House Bill 18) and Utah (Senate Bill 194), mandate the use of age-assurance technologies on platforms to restrict young users' access. Many new laws do not overtly mandate their implementation; however, their adoption could streamline compliance for online services, and thus, may be inadvertently encouraged. The OPC may want to consider this in the drafting of any regulation or guidance on the appropriate application of age-assurance systems in the digital environment.

The Children's Code and CAADCA are examples of regulatory interventions that do not mandate the use of age assurance. By requiring online services to provide enhanced privacy protections to users under a specific age, however, they allow online services to use age-assurance systems to estimate which users require heightened protections and which do not. The Children's Code is "not prescriptive" about which methods should be used to estimate or verify users' ages but requires that online services apply the Code's privacy-by-default standards to all users, regardless of their age, if age cannot be established with an appropriate level of certainty.²⁹

This is incorporated into the OPC's preliminary position, which states: "organizations should be required to justify why a particular age assurance technique is a more appropriate option than, for example, assuming all users are young people and applying appropriate practices." The OPC might consider expanding these requirements. Where feasible, the introduction of privacy-by-default standards for all online service users should be explored and encouraged to promote children's online safety before age assurance is implemented as a means of providing privacy-preserving features to child users only. This is supported by research showing that many adults are deeply concerned about platforms' data processing practices and would welcome more privacy protections in the digital environment.³⁰ A large cross-cultural study spanning the USA, UK, and Europe (n = 3,216) found that between 60-77% of participants objected to the collection and use of data related to their online communications, and between 55-69% objected to the use of their location history.³¹ This is underscored by a recent Pew Research study finding that 81% of Americans are concerned about companies' data collection practices, and 71% are concerned about the US government's.³² Indeed, 64% of Canadians have little to no trust in "big tech" to protect their personal information.³³

²⁹ "Age assurance for the Children's code," Information Commissioner's Office, 2024. [LINK](#)

³⁰ McClain, C., Faverio, M., Anderson, M., & Park, E. (2023). *Views of data privacy risks, personal data and digital privacy laws*. [LINK](#)

³¹ Kozyreva, A., Lorenz-Spreen, P., Hertwig, R., Lewandowsky, S., & Herzog, S. M. (2021). Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain, and the United States. *Humanities and Social Sciences Communications*, 8(1), 1–11. [LINK](#)

³² McClain et al., 2023

³³ Office of the Privacy Commissioner of Canada. (2023). *2022-23 Survey of Canadians on Privacy-Related Issues*.

The successful implementation of age-assurance systems in the digital environment requires public trust, which could potentially be enhanced by increased privacy protections for all service users, not just children. Some of the changes social media companies have made to their platforms to comply with the Children’s Code in the UK are restricted location history, limited personalized advertising, and the removal of user-to-user messaging for child users.³⁴ It is worth exploring whether these types of design changes, prompted by the introduction of new online safety regulations for children, would also be beneficial for and appreciated by adult users. If so, the circumstances in which age-assurance systems should be implemented online need to be carefully considered.

As outlined in the OPC’s preliminary position, the use of age-assurance systems should be restricted to situations that “pose a high risk to the best interests of young people” and “consider impacts on the privacy rights of both young persons and adult users of the online service.” This could be extended to include situations in which the potential harms to children from platform engagement are significant and well-evidenced. Crucial to this process is ongoing analysis of research that explores the impacts of digital technology use on children’s health and wellbeing and the potential harms associated with exposure to detrimental online content. This is because online safety legislation that is likely to instigate the implementation of age-assurance systems in Canada, such as the recently proposed Online Harms Bill, aims to protect children online primarily by reducing their exposure to harmful content.

Evaluating age-assurance systems involves examining the purpose and intended outcomes of the age-based online safety policies these technologies support. Research indicates that children respond to online content and interactions differently, with varying levels of sensitivity that can be influenced by developmental stage, gender,³⁵ and existing vulnerabilities, such as history of victimization³⁶ and attentional problems.³⁷ Early findings from our own ongoing longitudinal study of Canadian children’s attitudes toward age appropriateness in digital games shows that children “have their own thresholds and criteria for what is appropriate for them” in games, and this threshold is not based on numeric age alone.³⁸ The implementation of age-assurance systems in the digital environment should be preceded by a clear necessity for age-based online safety policies. This is crucial because individuals of the same age can face varying levels of risk when engaging in similar digital practices or consuming the same online content.

³⁴ NetChoice v. Bonta, Declaration of Emily Keane, Deputy Commissioner of Regulatory Policy for the ICO in Support of Defendant’s Opposition to Plaintiff’s Motion for Preliminary Injunction (2023). [LINK](#)

³⁵ Orben, A., Przybylski, A. K., Blakemore, S.-J., & Kievit, R. A. (2022). Windows of developmental sensitivity to social media. *Nature Communications*, 13(1), 1649. [LINK](#)

³⁶ Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. [LINK](#)

³⁷ George, M. J., Russell, M. A., Piontak, J. R., & Odgers, C. L. (2018). Concurrent and Subsequent Associations Between Daily Digital Technology Use and High-Risk Adolescents’ Mental Health Symptoms. *Child Development*, 89(1), 78–88. [LINK](#)

³⁸ Swerdfager et al., 2024

4. What complementary steps might the OPC consider taking to promote privacy and online safety for young people?

We are happy to read the OPC's position that age-assurance systems "should not require individuals to undergo an age assurance process to access non-restricted content." A vital complementary step is to clarify how "restricted" and "non-restricted content" will be defined and by whom. To date, outside of very specific examples where legal definitions outlining a minimum age are available (e.g., sexually explicit material), definitions and determinations of the age appropriateness of various types of content, interactions, and experiences have largely been left to the platforms and service providers to figure out for themselves: either individually or through self-regulatory systems managed by industry associations.

There is a long history of digital service providers establishing age restrictions in their terms of service agreements or privacy policies that bear little relationship to the actual contents of the services, or to the types of things we might assume go into considerations of age appropriateness, such as developmental readiness. Research shows that over the past two decades, numerous websites, platforms, games, and social networks have opted to ban children under 18 years or 13 years largely in order to avoid the additional costs and efforts associated with complying to children's privacy protection laws, such as the US-based Children's Online Privacy Protection Act (COPPA).³⁹ Age-assurance systems should never be implemented without careful consideration of why children below a certain age will be restricted from accessing the service or content. The reasons behind each and every age restriction should be clearly explained, evidence-based, and justifiable. Age restrictions should never be applied simply to avoid compliance to Canadian laws and policies, and this should be part of future clarifications of restricted and non-restricted content.

Notably, the decision in the 1990s to end COPPA protections at age 13 emerged after considerable debate and compromise between policymakers and industry groups. It is not based on scientific evidence of a particularly relevant (let alone) universal milestone in children's cognitive or emotional development at age 13, but rather its consistency with US cultural norms around adolescent independence, media ratings (e.g. films can be rated PG13, games rated T are for players 13 years and older, etc.), and the fact that the most 13 year-olds are able to distinguish between advertisements from other content.⁴⁰ These reasons do not translate all that well to the contemporary, let alone Canadian, context. There is a movement underway in the US to expand privacy protections to teenagers as well as younger children, which aligns more closely to the Children's Code, the UNCRC, and other guidelines and policies. This movement draws on substantial research showing that teens would benefit from enhanced privacy protections, something that most teens say is a high priority for them.⁴¹

³⁹ Grimes, S.M. & Fields, D.A. (2012). *Kids online: A new research agenda for understanding social networking forums*. New York. The Joan Ganz Cooney Center at Sesame Workshop. [LINK](#)

⁴⁰ Jargon, Julie (2019, June 18). How 13 became the Internet's age of adulthood. *Wall Street Journal*. [LINK](#)

⁴¹ Third, A., & Moody, L. (2021). *Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25*. 5Rights Foundation. [LINK](#)

Of course, and in keeping with our previous responses, it is important to remember that there are vital differences among and across age groups, and that the best interests of individual children and teens must always be considered as new protections are designed and implemented, with an emphasis on their privacy and multiple other rights. The OPC already acknowledges that teens also warrant special considerations in the definition of “young people” provided in the position statement. However, the inclusion of teenagers and children of younger ages should be clarified and differentiated in future policy and guidance work.

Summary of Recommendations

We encourage the OPC to:

1. Consider commissioning research that consults children of diverse ages about age-assurance systems to help ensure that any policy or guidance developed is child-inclusive and reflects the real needs and concerns of young Canadians.
2. Introduce special provisions for the processing of biometric data during age assurance processes because unlike other forms of personal information, biometric data are unique, unalterable, and comprehensive. Privacy risks are significantly heightened when biometric data are compromised.
3. Explore the privacy risks arising from age assurance processes that are not a consequence of identification. While identifiability is a high-level impact of age assurance, it is not the only privacy risk associated with the collection of citizens’ demographic and behavioural data by these systems. The use of personal data collected during age assurance processes for the development or optimization of AI tools poses significant threats to citizens’ autonomy and self-determination which require analysis.
4. Encourage online services to adopt privacy-by-default standards for all service users prior to implementing age-assurance systems that distinguish children from adults for the purposes of providing privacy-preserving features to child users only.
5. Pursue high-quality evidence that demonstrates the need for age restrictions in digital environments before developing guidance on best practices for implementing age-assurance systems that restrict or limit children’s access to online content or services.
6. Clarify how “restricted” and “non-restricted content” will be defined and by whom to support the development of age restrictions in online spaces that are evidence based and reflective of children’s developmental readiness.