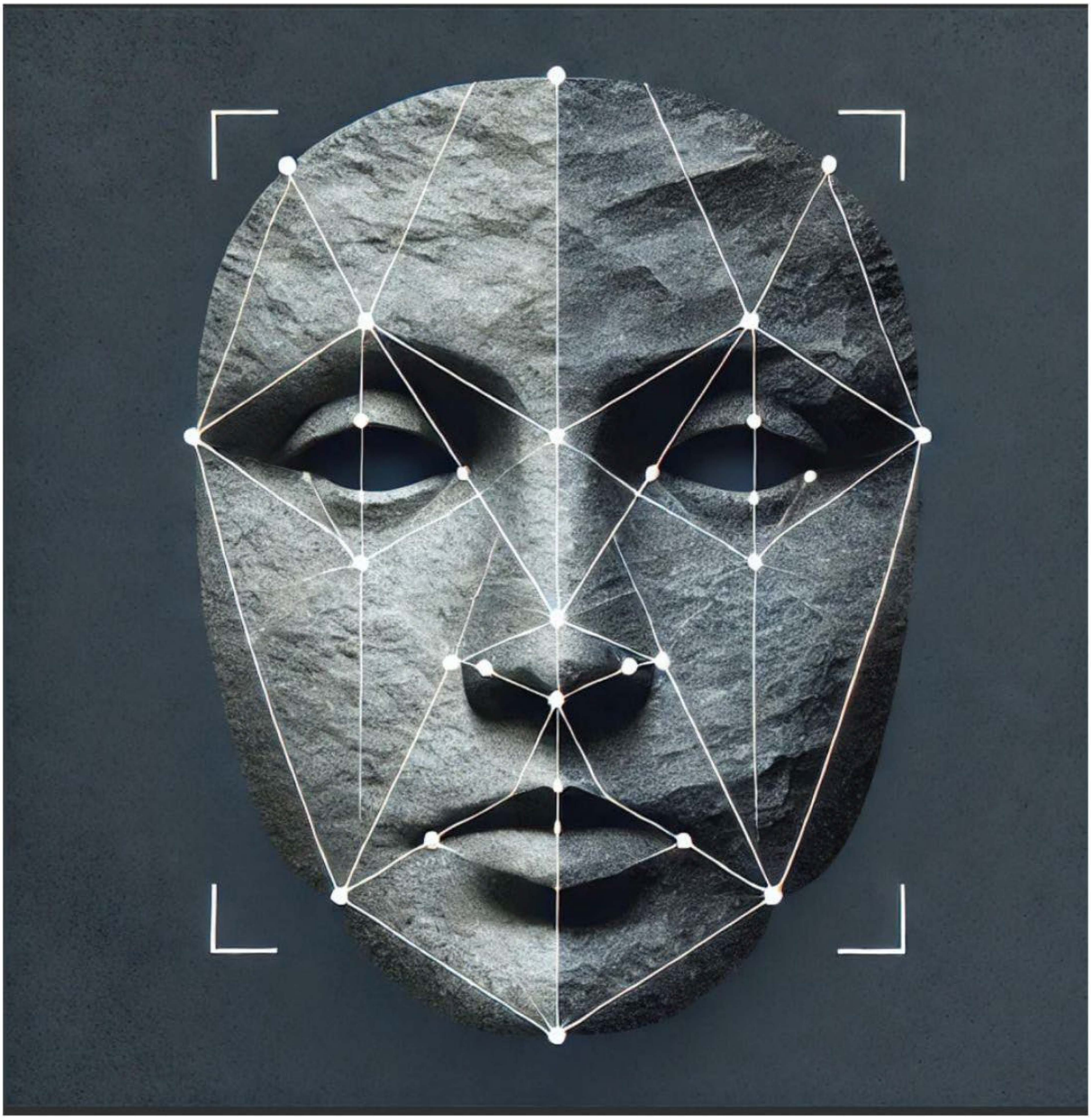
Ready for Prime Time?

Are Age Assurance Systems Sophisticated Enough to Verify Users' Age Without Breaching their Privacy Rights?



A submission to the Office of the Privacy Commissioner's Consultation on Age Assurance by Eve Gaumond, David Fewer, Sarah Scheffler, Madelyne Xiao, Pierre-Luc Déziel and Melissa Dupuis-Crane for

CIPPIC

Cover page photo credit: Jan Canty, creative commons on unsplash (modified by the author through ChatGPT).

CIPPIC—the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic—is a legal clinic based at the University of Ottawa's Faculty of Law. Its mandate is to advocate for the public interest on matters arising at the intersection of law and technology.

This submission was prepared by the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University of Ottawa. This document is intended for informational purposes only and should not be interpreted as legal advice. For inquiries or further information, please contact admin@cippic.ca.

AUTHORS

Eve Gaumond
PhD Student, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic and Université de Montréal's CIFAR Chair on AI and Human Rights

David Fewer
Director & General Counsel, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

Sarah Scheffler
Assistant Professor, Software and Societal Systems, Carnegie Mellon University

Madelyne Xiao
PhD Candidate, Department of Computer Science, Princeton University

Pierre-Luc Déziel
Full Professor, Faculty of Law, Université Laval

Melissa Dupuis-Crane
Articling Student, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

EXECUTIVE SUMMARY

Our submission questions the assumption that age assurance systems in today's marketplace have reached a state of sophistication sufficient to effectively ascertain users' age without breaching privacy rights. In so doing, we offer a tentative definition for "designing and using age assurance systems in a privacy protective manner."

We suggest that truly privacy-preserving age assurance systems must:

- guarantee anonymity;
- be effective; and
- demonstrably comply with Canadian data protection laws.

To better understand if existing systems meet this definition, we have designed a summary assessment tool inspired by existing privacy impact assessment models and industry standards. The tool is a questionnaire comprising fifteen questions. These questions build on the work of privacy commissioners and standards organizations such as ISO and IEEE. We have designed the tool to elicit information needed to assess whether an age assurance system meets the three requirements set out in the definition.

Members of our team are currently working on testing whether the leading players in the age assurance market meet this definition. We expect preliminary results in the following weeks. We will share these results with the Office of the Privacy Commissioner as they become available.

1. What is a Privacy Protective Age Assurance System?

To determine if an age assurance system is *used and designed* in a privacy protective manner, we first need to define what it means to *offer* age assurance services in a privacy-protective manner. We have synthesized existing frameworks to devise a tentative definition: privacy-protective age assurance systems must (1) guarantee user anonymity, (2) be effective, and (3) demonstrably comply with Canadian data protection laws.

The first requirement, anonymity, derives from Canadian jurisprudence, which protects online anonymity as a fundamental right.[1] This requirement also aligns with the Spanish Data Protection Agency's Decalogue of *Principles for Age Verification and Protection of Minors from Inappropriate Content*, which states that age verification systems "must guarantee that the identification, tracking, or location of minors over the Internet is impossible".[2] The second requirement, effectiveness, is rooted in the Office of the Privacy Commissioner's "appropriate purpose" test provided at 5(3) of PIPEDA which in restricting dealings with personal information to "appropriate" purposes by definition excludes "ineffective" systems.[3] It is also supported by section 11(2)(c) of the proposed *Act to restrict young persons' online access to sexually explicit material* (S-210), which would require age verification systems to be reliable, and by the *Spanish decalogue* which requires that age verification be carried out accurately.[4] Finally, the last requirement, legal compliance, is an open-textured provision that captures a broad range of infringements on data protection rights. It mirrors the substance of S-210's privacy provision as it also requires that age assurance systems maintain user privacy, protect personal information, collect, and use personal data solely for age-verification purposes (except where required by law), and destroy any personal information once verification is completed. Additionally, it opens the possibility of sanctioning other data protection violations not covered by S-210.

To better understand if existing systems meet this definition, we have designed a summary assessment tool inspired by existing privacy impact assessment models and industry standards. The tool is a questionnaire comprising fifteen questions. These questions derive from the work of privacy commissioners and standards organizations such as ISO and IEEE. We have designed the tool to elicit information needed to assess whether an age assurance system meets the three requirements set out in the definition.

---

[1] *R v Spencer*, 2014 SCC 43. [*Spencer*]

[2] Agencia Española Protección Datos, *Decalogue of principles: Age verification and protection of minors from inappropriate content* (December 2003).

[3] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 5(3).

[4] Bill S-210, *An Act to restrict young persons' online access to sexually explicit material*, 1st Sess, 44th Parl, 2023, c 11(2)(c) (as passed by the Senate April 18 2023).

1.1 Privacy Protective Age Assurance Systems Must Preserve Anonymity

Living free from surveillance is a fundamental right.[5] One of its components, the right to anonymity protects the freedom to be seen without being identified. Anonymity is the state of privacy that allows people to experience a sense of freedom and relaxation in the public sphere.[6] It's the reason why festival goers dance freely in large crowds—because *what they do* can't be associated with *who they are*.[7] It promotes human growth and flourishing by allowing people to try new experiences and engage with different ideas without being held accountable for everything they do, say or think.[8] All in all, it is a necessary condition to freedom and autonomy, as it gives people space to reflect on the kind of person they want to be and the kind of life they want to live.[9]

Canadian courts have confirmed on several occasions that the law protects anonymity both online and offline.[10] Police officers can't force people to identify themselves in the street if they haven't done anything wrong, and what people do on the internet can't be linked back to them except if there are reasons to believe that they're engaging in criminal activities or civil wrongs.

Requiring internet users to provide identity documents to access certain websites would threaten the right to anonymity online. If Canada decides to move forward with the implementation of age assurance systems to access certain websites, it must distinguish two concepts that are often muddled: identification and authorization. Identification involves disclosing who you are. Authorization, on the other hand, only involves proving that you are allowed to do something.[11] While identification and authorization are often conflated—alcohol vendors use IDs to prevent minors from purchasing alcohol, for instance—they can also be employed as independent mechanisms. Consider: there is more than one way to get access to a building: you can have a key (authorization), the doorman can let you in because he knows who you are (identification), or you can have a card with your name and picture on it that you scan to get in (identification + authorization).

Similarly, it is also possible to disentangle authorization and identification in the context of providing access to stigmatizing items and content. The city of San Francisco, for instance, developed an anonymous system for its medical marijuana program. The city granted users a card designed with anonymity in mind: except for an authenticating picture, the card contained

---

[5] *R v Duarte*, 1990 CanLII 150 (SCC); *R v Wong*, 1990 CanLII 56 (SCC); Office of the Privacy Commissioner of Canada, "Privacy guidance on facial recognition for police agencies" (2 May 2022), online: <https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/>.

[6] *R v Jarvis*, 2019 SCC 10.

[7] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 31-32.

[8] *R v Ward*, 2012 ONCA 660 at para 71. [*Ward*]

[9] Beate Rössler, *The Value of Privacy*, translated by R D V Glasgow (Cambridge, UK: Polity Press, 2005) at 73.

[10] *R v Greaves*, 2004 BCCA 484 at para 50; *Spencer*, *supra* note 1; *Ward*, *supra* note 8; *R v Bykovets*, 2024 SCC 6.

[11] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus Books, 2003) at 184.

no identifying information.[12] The Spanish Data Protection Authority similarly designed a system for preventing minors from accessing inappropriate content online that renders the identification, tracking or location of minors impossible.[13]

Canada should follow the same path. When it comes to limiting access to certain content, the only forms of age assurance justifiable in a free and democratic society are those that rely solely on authorization—and thus preserve anonymity. This aligns with the OPC's past positions regarding privacy and identity stating that Parliament should promote anonymity as the norm in law.[14] It also aligns with the OPC's jurisprudence and that of provincial privacy commissioners which restrict practices of scanning physical IDs.[15]

We designed the questions below to help gather information to determine whether an age assurance system preserves anonymity.

Does the Age Assurance System Preserve Anonymity?	
1.	*What personal information ("PI") is collected, stored, and used?*
2.	*Is this PI necessary to conduct age verification?*
3.	*Is the PI "need to have" (as opposed to a "nice to have"?) to conduct age verification?*
4.	*What measures prevent reidentification?*
5.	*How will the system's user dispose of the PI?*

[12] *Ibid*.

[13] Agencia Española Protección Datos, *Decalogue of principles: Age verification and protection of minors from inappropriate content* (December 2003) at 7; Agencia Española Protección Datos, *Technical note: Description of the proofs of concept of systems for age verification and protection of minors from inappropriate content* (December 2003).

[14] Office of the Privacy Commissioner of Canada, "Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada" (24 October 2022) online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_220921_02/>; Office of the Privacy Commissioner of Canada, "Data at Your Fingertips Biometrics and the Challenges to Privacy" (February 2011) online: <https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/>; Office of the Privacy Commissioner of Canada, "Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues" (January 2008) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2008/id_paper/>.

[15] Office of the Privacy Commissioner of Canada, "Identification machines and video cameras in bars examined" (6 August 2010) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/pipeda-2008-396/>; Office of the Privacy Commissioner for British Columbia, "PIPA Order P09-01" (21 July 2009) online: <https://web.archive.org/web/20101227064247/https://www.oipc.bc.ca/PIPAOrders/2009/OrderP09-01.pdf>; See also *Highway Safety Code*, CQLR c C-24.2 at s 61.

1.2 Privacy Protective Age Assurance Systems Must be Effective

Collecting, using or disclosing personal information is only allowed when the purpose of the data processing is one that a reasonable person would consider appropriate in the circumstances.[16] Courts have developed a test to determine whether a given data processing pursues an appropriate purpose.[17] The test requires the data processor to identify the purpose of the data processing, and show that it is both necessary to accomplish the stated purpose and likely to be effective in accomplishing that purpose.[18] Effectiveness is thus a precondition for processing data legally. Using data in ways that are unlikely to meet the purpose for which they were collected constitutes a violation of the federal data protection regime. Therefore, the probable effectiveness of the age verification solutions must be demonstrated before they can be used legally in Canada.

There are two ways of approaching the effectiveness question. The first is to assess the effectiveness of the measure, i.e. determining if requiring age verification online protects minors from online harms. The alternative way is to focus on the effectiveness of the technology itself, i.e. testing if age assurance systems can verify internet users' age with sufficient accuracy. Given that our goal with this submission is to evaluate the claim that age assurance systems are ready for prime time, our analysis focuses on the latter.[19]

Information about the effectiveness and accuracy of commercial or public age assurance systems is scarce.[20] Very little information is available regarding their performance on children, and we are not aware of any research measuring their effectiveness against adversarial attacks.[21] The most comprehensive study about age verification/estimation systems was produced by the American National Institute of Standards and Technology (NIST). Unfortunately, NIST didn't measure how systems perform when users try to circumvent them by using disguises, cosmetics, or other kinds of presentation attacks, and its testing of the system' effectiveness on users under 14 was done only on a geographically homogeneous

---

[16] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 5(3).

[17] *Turner v Telus Communications Inc*, 2005 FC 1601 at para 48; *Eastmond v Canadian Pacific Railway*, 2004 FC 852 at para 13.

[18] Office of the Privacy Commissioner of Canada, "Employee objects to company's use of digital video surveillance cameras" (23 January 2003) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-114/>.

[19] However, it is worth highlighting that the effectiveness of age verifications requirements is scientifically contested. See *Free Speech Coalition et al v Paxton*, 95 F (4th) 263 (5th Cir 2024) in which Judge David A. Ezra makes a careful review of scientific evidence and experts testimony before concluding: "Based on the evidence in the parties' briefing, declarations, and hearing testimony, it is clear that age verification is considerably more intrusive while less effective than other alternatives."

[20] EDRi has produced a chart comparing the effectiveness of 11 different age verification methods. While it provides an interesting overview, it lacks data on how the effectiveness was assessed. See European Digital Rights, *Position paper: Online age verification and children's rights* (Brussels: EDRi, 2023); Age Check Certification Scheme's report, for its part, relies only on self-declared data. See Tony Allen et al, *Measurement of Age Assurance Technologies: Part 2 – Current and short-term capability of a range of Age Assurance measures* (UK: AVID Certification Services Ltd, 2023).

[21] The only performance data available for children comes from the age assurance providers themselves. There are performance discrepancies between self-reported data and data from independent auditors. See for instance Yoti, "Why do Yoti facial age estimation results published by NIST differ to those reported by Yoti in its white papers" (20 June 2024) online: <https://www.yoti.com/blog/comparing-yoti-age-results-with-nist/>.

dataset of mostly Mexican people.[22] In other words, the NIST study does not provide information on effectiveness across races for children nor does it provide information about effectiveness against attempts to spoof the systems.

For the moment, the standard method for age verification online is self-reporting. Typically, self-reporting asks users to choose their birth year from a dropdown menu, or to check a box to confirm that they are older than a certain age. From a privacy standpoint, these methods are non-invasive, and if users are honest, they work well. Issues only arise when users are interested in pretending they are older than they are. This is why it is important to test the effectiveness of age assurance systems under adversarial attacks. Moving away from the status quo and requiring new types of age assurance systems is not warranted if the new methods increase privacy risks without being more effective.

Canada should not move forward with stricter age assurance without having a more thorough understanding of how effective the technology is. Past experiences in testing the effectiveness of applications that are influenced by both social and technical factors have shown that establishing effectiveness targets in advance is critical.[23] The most telling example in that regard is the COVID Alert App. The team responsible for evaluating the app struggled to arrive at a determinative conclusion on effectiveness because of the lack of predetermined indicators.[24] In light of that, the evaluation report highlighted the need to set effectiveness and accuracy targets in advance as one of its key lessons learned.

As to age assurance systems, the only existing benchmarks are those developed by standards organizations such as ISO and IEEE. While these initiatives are important, they lack democratic legitimacy. Standards organizations are mostly led by the industry and the industry alone should not be tasked with setting performance metrics for technologies as impactful as age assurance systems. In Australia, the e-commissioner recommended holding public consultations involving children, parents, tech platforms, digital rights advocacy groups, researchers, and NGOs before passing laws mandating age verification online.[25] The e-commissioner also highlighted the need for comprehensive and transparent evaluations of age assurance systems—including assessment of accuracy and effectiveness—to inform these public consultations. The OPC should follow suit and advocate for public consultations informed by a more comprehensive assessment of age assurance systems' effectiveness and accuracy.

---

[22] See Kayee Hanaoka et al, *Face Analysis Technology Evaluation: Age Estimation and Verification* (Gaithersburg, MD: National Institute of Standards and Technology, 2024) at 6: "We use a set of visa photos collected in one country, Mexico, to quantify age estimation accuracy in children between age 0 to 17"; See also Mei Ngan & Patrick Grother, *Face Recognition Vendor Test: Performance of Automated Age Estimation Algorithms* (Gaithersburg, MD: National Institute of Standards and Technology, 2014) at 10: "The DoS/Natural dataset contains a subset of 6,172,395 images over an ethnically-homogeneous population spanning ages."

[23] Office of Audit and Evaluation Health Canada and the Public Health Agency of Canada, "Evaluation of the National COVID-19 Exposure Notification App" (June 2022) online: <https://www.canada.ca/en/health-canada/corporate/transparency/corporate-management-reporting/evaluation/covid-alert-national-covid-19-exposure-notification-app.html#a45>.

[24] *Ibid*.

[25] eSafetyCommissioner, *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography* (Australia: Australian Government, 2023) at 29.

The consultation could take the form of a citizen assembly. Citizens assemblies are long-form deliberative processes where randomly selected citizens gather to learn about complex issues to provide recommendations to public authorities. Citizens' assemblies typically tackle divisive issues that involve trade-offs or compromises such as abortion or climate change.[26] Canada has been experimenting with citizens' assemblies in the digital sphere by holding citizen assemblies on democratic expression and digital rights for youth.[27]

To inform these deliberations, additional data about the effectiveness and accuracy of age assurance systems is needed. Existing age assurance systems should be subjected to adversarial checks to assess performance in the context where a user is actively attempting to circumvent the age assurance mechanism. That means testing accuracy when users are showing doctored IDs or wearing disguises to appear older, for instance. There is also a need for more data regarding the performance of age evaluation systems on minors, especially those slightly older or younger than the age limit. How effective are these systems at evaluating if 17-year-olds are allowed to access the content they are seeking? The way the incertitude regarding users who fall in that ambiguous age category is managed is also an issue that should be more thoroughly studied and discussed. If systems are not capable of accurately evaluating how old they are, are users slightly older than the age limit required to show ID? Finally, all these tests should be realized with fairness in mind. Given the well-known bias of certain kinds of age assurance systems, false positive and false negative rates should be measured across race, age, and gender. Error parity metrics should also be assessed to ensure that protected groups are not disproportionately affected by inaccuracies.[28] Finally, fairness should include socio-economic considerations—some tests should be conducted to measure how effective age assurance systems are on older devices with low quality cameras for instance.

The questions below are designed to inform the discussion regarding effectiveness. While they do not provide a precise answer as to what "effective enough" means, they are designed to foster the conversation and provide useful information to inform eventual public debate.

Is this Age Assurance System Effective?	
6	*Consider the data set used to test the system: is it representative of the users' population and real-world use conditions?*
7	*How does the system's performance compare to industry standards of accuracy under normal conditions?*

[26] 3rd Canadian Citizens' Assembly on Democratic Expression, *Canadian Citizens' Assembly on Democratic Expression: Recommendations for reducing online harms and safeguarding human rights in Canada* (Ottawa: Public Policy Forum, 2022).

[27] *Ibid*; David Kenny & Aileen Kavanagh, "Are the People the Masters? Constitutional Referendums in Ireland" in Richard Albert & Richard Stacey, eds, *The Limits and Legitimacy of Referendums* (OUP, 2020); Canadian Youth Assembly on Digital Rights and Safety, *Canadian Youth Assembly on Digital Rights and Safety: Recommendations to promote the safety, well-being and flourishing of Canadian youth online* (Montreal: Centre for Media, Technology and Democracy, 2023).

[28] Kayee Hanaoka et al, *Face Analysis Technology Evaluation: Age Estimation and Verification* (Gaithersburg, MD: National Institute of Standards and Technology, 2024)

8	*How does the system's performance change from normal conditions when facing attackers with minimal time and financial resources (1 minute and US $10 per attempt)?*
9.	*How does the system's performance change from normal conditions for users that are (less than) 2 years over/under the age limit?*
10	*How do the error rates vary for users from protected groups and marginalized groups?*

1.3 Privacy Protective Age Assurance Systems Must be Demonstrably Compliant with Data Protection Laws.

Age assurance systems handle particularly sensitive information—especially when they are used to control access to pornographic material. When they function as gatekeepers for adult websites, they are the nexus between biometric data and information that carries reputational risks. Given the sensitivity of the information they process, age assurance companies should comply with the most stringent standards applicable in terms of data protection.

The failure to comply with heightened data protection standards could cause significant harm. The Ashley Madison data breach offers just a glimpse of what this harm could look like. In 2015, the affair-facilitating website suffered a data breach. The breach resulted in the details of thirty-six million accounts being published online. Users whose personal information was revealed have suffered reputational harm and some of them were targeted by extortion schemes.[29] The OPC found that the security safeguards in place when the breach occurred were not proportionate to the sensitivity of the information at stake.[30] Despite its findings, the OPC couldn't impose sanctions. Given the difficulty of holding those who fail to comply with data protection principles accountable, it is not clear that the framework governing data protection in Canada is robust enough to meaningfully protect Canadians from the risks associated with age assurance systems, which are even greater than those associated with the Ashley Madison scandal.

Therefore, age assurance systems should not be deployed in Canada if there are no additional data protection requirements built into the regime. To strengthen the regime, the priority should be on reinforcing accountability mechanisms rather than making substantive changes to existing data protection principles. Indeed, on the substance, the federal data protection regime is satisfactory. Its real problem lies in the complexity of sanctioning those who fail to comply with it. For instance, under PIPEDA, age assurance companies would already have to comply with the most stringent understanding of the limitation principle. That is to say that they would

[29] Emily Laidlaw, "Technology Mindfulness and the Future of the Tort of Privacy", 2023 60-3 Osgoode Hall Law Journal 597.

[30] Office of the Privacy Commissioner of Canada, "Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner" (2016) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/>.

already be required to collect, use, share and store data for age verification purposes only. The problem here is that what is necessary for age verification purposes can be contentious and companies could exploit this loophole to reuse or sell data for purposes loosely related to age verification without being held accountable.

To overcome this issue, we propose to include the obligation of demonstrably complying with data protection principles into the definition of a privacy preserving age assurance system. This requirement would force companies to document their compliance with the most stringent understanding of data protection principles and prevent them from trying to avoid sanctions by arguing that they thought they had to comply with lower standards. Demonstrating compliance could be done through the OPC's privacy management program or a similar process.[31]

This kind of ex-ante measure is typical of the current wave of regulations governing new technologies. It helps prevent harm before it occurs by forcing companies to show that they are taking measures to mitigate risks. Among other things, demonstrating compliance with data protection laws would require age assurance companies to document the purposes for which they process personal information and the amounts and types of information needed to fulfill that purpose; to share their policy regarding the deletion of information that is no longer required to fulfill identified purposes; and to explain how their information security practices are proportional to the sensitivity of the information they process.

Below is a non-exhaustive list of questions that age assurance companies must address when demonstrating compliance with data protection laws. We have designed the questions to assess whether age assurance companies ensure that they do not use the data they collect for purposes other than age assurance. We focus on this risk because it is the one which is most likely to cause harm in the current context. However, other questions associated with other data protection principles would also be worth exploring.

Does this System Comply with Canadian Data Protection Laws?	
11	*What PI does the system store or share, with whom, and for what specific purpose?*
12	*Why is storing or sharing this PI necessary to conduct the age verification service?*
13	*In what form and format does the service retain the PI, and for how long?*
14	*Has the service employed industry-standard security and access controls to prevent loss, theft, or unauthorized access, use, disclosure, copying, or modification of PI, both in transit and at rest?*
15	*What are the mechanisms in place to detect and respond to breaches?*

[31] Office of the Privacy Commissioner of Canada, "Getting Accountability Right with a Privacy Management Program" (2012) online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/>.

EVALUATION TOOL

The ambitions of this tool are modest. This is not meant to be a thorough analysis of the privacy implications of existing age assurance systems, but rather an exploratory tool aiming to inform public deliberations.

Does the Age Assurance System Preserve Anonymity?	
1.	*What personal information ("PI") is collected, stored, and used?*
2.	*Is this PI necessary to conduct age verification?*
3.	*Is the PI "need to have" (as opposed to a "nice to have"?) to conduct age verification?*
4.	*What measures prevent reidentification?*
5.	*How will the system's user dispose of the PI?*
Is this Age Assurance System Effective?	
6	*Consider the data set used to test the system: is it representative of the users' population and real-world use conditions?*
7	*How does the system's performance compare to industry standards of accuracy under normal conditions?*
8	*How does the system's performance change from normal conditions when facing attackers with minimal time and financial resources (1 minute and US $10 per attempt)?*
9.	*How does the system's performance change from normal conditions for users that are (less than) 2 years over/under the age limit?*
10	*How do the error rates vary for users from protected groups and marginalized groups?*
Does this System Comply with Canadian Data Protection Laws?	
11	*What PI does the system store or share, with whom, and for what specific purpose?*
12	*Why is storing or sharing this PI necessary to conduct the age verification service?*
13	*In what form and format does the service retain the PI, and for how long?*
14	*Has the service employed industry-standard security and access controls to prevent loss, theft, or unauthorized access, use, disclosure, copying, or modification of PI, both in transit and at rest?*
15	*What are the mechanisms in place to detect and respond to breaches?*