Making Privacy More than a Virtual Reality

The Challenges of Extending Canadian Privacy Law to Extended Reality

CIPPIC

Making Privacy More than a Virtual Reality: The Challenges of Extending Canadian Privacy Law to Extended Reality

Report of the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) to the Office of the Privacy Commissioner's Contributions Program

Cover page. Photo credit: Giu Vicente on Unsplash

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 report and corresponding material were prepared by the **Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic** (CIPPIC) at the University of Ottawa and funded by the **Office of the Privacy Commissioner's Contributions Program** for the project entitled: "Making Privacy More than a Virtual Reality: The Challenges of Extending Canadian Privacy Law to Extended Reality." This document is intended for informational purpose only and should not be interpreted as legal advice. For inquiries or further information, please contact admin@cippic.ca.

CIPPIC staff and collaborative researchers Emily Chu, Renae Pennington, Chloe Bechard, Shaarini Ravitharan, Harmon Imeson Jorna, Eve Gaumond and Drew May contributed to this project under the lead of project administrator Christian Clavette.

Acknowledgements

This report on the privacy implications of extended reality (XR) technologies in Canada stands as a testament to the collaborative effort and dedication of a wide range of contributors, whose expertise and insights have been invaluable to the depth and breadth of our analysis. We extend our sincerest gratitude to all those who have generously shared their time, knowledge, and resources to make this comprehensive study possible.

Special acknowledgements go to Professor Vivek Krishnamurthy for initiating this project and providing invaluable guidance. We also appreciate Professor Teresa Scassa's leadership in navigating AI and XR challenges and Professor Brittan Heller's early feedback.

Our gratitude extends to stakeholders from academia and industry, including Professors Jacquie Burkell, Leslie Regan Shade, Jane Bailey, Valerie Steeves, and industry professionals Chantal Bernier, Caroline Dupuis, Matthew Sheardown, and Alex Gimson.

Lastly, we thank our dedicated student interns Emily Chu, Renae Pennington, Chloe Bechard, Shaarini Ravitharan, Harmon Imeson Jorna, Eve Gaumond and Drew May for their professionalism, innovative ideas, and hard work in researching, analyzing, and compiling this report.

Table of Contents

Executive Summary

Emerging virtual and extended reality technology is testing the bounds of Canada's privacy laws. While the technology is poised to race into a new frontier in immersion and practical uses, Canadian laws are struggling to keep pace with proper privacy protections.

XR is an umbrella term that encompasses three types of technology that offer different levels of immersion: augmented reality (AR), virtual reality (VR) and mixed reality (MR). This report focuses mainly on XR headsets like the Apple Vision Pro, a relatively new entrant into the marketplace that creates a three-dimensional user experience through a mix of sensors, cameras, microphones and gyroscope. XR devices use hand and eye tracking to enable the user to control the device while an array of sensors, including built-in cameras, map the user's environment and track their movements.

These technologies' privacy concerns are not unique, but the bundling of privacy concerns with XR devices is unprecedented. The headsets collect a vast amount of sensitive biometric data, which in-turn can be used to infer private personal information about the headset wearer. The devices can also gather information about the people around the user, often without their consent. These issues combine to create situations not fully contemplated under Canadian privacy law.

Canada currently has a patchwork of privacy and data protection laws. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs data processing in the private sector, but Alberta, British Columbia and Quebec have provincial laws that supersede it in certain contexts. PIPEDA is also on the cusp of being replaced by the *Consumer Privacy Protection Act* (CPPA), which seeks to update and modernize the legislation.

This report evaluates XR technologies through the lenses of Canada's current privacy legislation, PIPEDA, and the legislation proposed to replace it, the CPPA. CIPPIC undertook extensive interviews with academics and industry stakeholders, and analyzed the legislation, the technology, and related privacy policies. CIPPIC proposes three key legal recommendations to address XR's privacy challenges:

- PIPEDA should require explicit consent for collecting and using user data, along with a detailed explanation of how the platform intends to use it.
- The Office of the Privacy Commissioner should adopt a co-regulatory model where the OPC and XR technology stakeholders find a consensus for compliance with the law's requirements for commercial actors.
- Going forward, the federal government should amend the CPPA before it comes into force to define "sensitive information" in the Act, centre consent on the user, and strengthen protections for children.

Legal rules, alone, will not be enough to address the privacy challenges presented by XR. The OPC should adopt a multi-faceted approach to addressing the privacy challenges of these technologies. The OPC could also increase privacy education for both users and developers, introduce a privacy grading system or adopt a comply-or-explain enforcement model to address broader privacy concerns around XR. These measures would help address many of the privacy concerns raised in this report. XR technology offers amazing potential benefits in entertainment, education and business — it just shouldn't come at the expense of Canadians' privacy.

Introduction

This report is the result of a collaborative work that involved academics, industry professionals and students. It was funded through the Contribution Program of the Office of the Privacy Commissioner of Canada. It examines whether Canadian law is well equipped to deal with the privacy challenges posed by extended reality technologies (XR), particular attention paid to children's privacy issues.[1]

To explore these issues, CIPPIC conducted eight semi-directed interviews with stakeholders from academia and industry.[2] On the academic side, we interviewed professors from the fields of law, criminology and information and media studies. On the industry side, we interviewed three employees working in two different XR companies and a lawyer in private practice whose clients include tech companies, financial institutions, biotech companies, data analytics firms and government institutions.

This report is informed by what we heard during these interviews. It tackles four main questions:

- What is extended reality?
- How does extended reality impacts privacy?
- Is Canadian law well equipped to protect XR Users?
- What does CIPPIC suggest to better protect Canadians interacting with XR?

[1] The most comprehensive studies on XR consider XR technology from the perspective of European and American law, respectively. See Emil Albihn Henriksson, "Data Protection Challenges for Virtual Reality Applications" (2018) 1:1 Interactive Entertainment L Rev; see also Yeji Kim, "Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent" (2022) 110:1 Cal L Rev; Brittan Heller, "Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law" (2020) 23: 1 Vanderbilt J Entertainment & Tech L; Suchismita Pahi & Calli Schroeder, "Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy is Several of Them" (Forthcoming 2023) 4 Notre Dame J Emerging Tech; Mark A Lemley & Eugene Volokh, "Law, Virtual Reality, and Augmented Reality" (2018) 166: 5 U Pa L Rev.

[2] The questionnaire and the participant's bios are available in the Appendix.

1. What is Extended Reality?

XR is an umbrella term that encompasses three main types of technologies: augmented reality, virtual reality, and mixed reality:

> **Augmented Reality (AR)** overlays digital information onto the real world. For example, AR can be used in applications like Pokémon Go, where virtual characters appear in the real world through a smartphone screen. In addition to smartphones and tablets, there are also AR glasses which use cameras and sensors to detect the environment and place virtual objects, animations, or data over the physical surroundings. Ray-Ban Meta smart glasses, for example, have embedded AI assistant software and allow users to directly post multimedia content to the company's Instagram and Facebook properties.
>
> **Virtual Reality (VR)** immerses users in a completely virtual environment. VR headsets like the Oculus Quest, for instance, use screens, motion sensors, and gyroscopes to track head and hand movements, allowing users to navigate and interact within a 3D digital space. This kind of technology is used for applications ranging from gaming to virtual tours and medical training simulations.
>
> **Mixed Reality (MR)** devices, such as Apple's Vision Pro and Meta's Quest 3, represent the latest advancements in XR technology. These devices combine the capabilities of both VR and AR, allowing users to seamlessly transition between augmented and virtual environments. The Vision Pro, for example, uses LiDAR scanners, multiple cameras, and advanced eye-tracking technology to create an immersive MR experience. These sensors enable the device to understand the user's environment and interact with it dynamically, providing a more natural and intuitive user experience.

While XR first emerged in the 1960s, systems back then were bulky, expensive, and limited by the technology of the time, featuring low-resolution displays and limited motion tracking capabilities. It was not until the early 2010's that the technology as we know it today really began to blossom. Leading the way was the Oculus Rift which revolutionized VR by providing high-quality, immersive experiences at a relatively affordable price.

Since then, XR has kept improving. Modern systems, such as the Oculus Quest 2 and Apple Vision Pro, have become standalone devices that no longer need to be tethered to external computers. These devices incorporate onboard processing power and cloud computing to enhance performance

and user experience. They use an array of sensors, including built-in cameras, to map the user's environment and track their movements without the need for external sensors.

A basic XR headset like the Oculus Quest 2 works by combining several key components. It has high-resolution screens that are placed close to the user's eyes, providing a wide field of view. These displays are split to show slightly different perspectives to each eye, creating a stereoscopic 3D effect. The headset uses internal sensors, including gyroscopes, accelerometers, and magnetometers, to track head movements and adjust the display in real-time to match the user's perspective. The next paragraphs explore how these components interact to create an immersive experience for users.

Eye tracking enhances the immersive experience by monitoring where the user is looking. This technology uses infrared sensors and cameras inside the headset, pointed at the face, to track the movement of the user's eyes. By determining the precise direction and focus of the gaze, the system can render portions of the virtual environment in higher resolution where the user is looking—this technique is known as foveated rendering. This not only improves visual quality but also reduces the device's computational load, allowing for more efficient processing power. Eye tracking can also be used for intuitive control interfaces, enabling users to interact with menus and objects simply by looking at them.

Pupillometry is the measurement of pupil size and reactivity. It's an integral aspect of eye-tracking technology in XR systems. It provides insights into the user's cognitive and emotional state by analyzing changes in pupil diameter in response to stimuli, helping to create more personalized and responsive XR experiences. When integrated with eye tracking, pupillometry uses the same infrared sensors and cameras to detect and measure the pupil's response to various visual and environmental factors. This integration allows the device to adjust lighting, focus, and other elements in real-time based on the user's physiological responses, enhancing the overall immersive experience.

Inside-out tracking in VR headsets involves using cameras mounted on the headset itself to observe and map the surrounding environment. These cameras capture the physical space. They detect features such as walls, furniture, and other objects. The software then creates a virtual map of the environment, which is used to track the user's movements within that space. This method eliminates the need for external sensors or beacons, providing greater freedom of movement and a more streamlined setup process. The cameras also track the position and orientation of

the headset, allowing the virtual environment to adjust dynamically as the user moves.

Hand tracking is also a feature of some devices like the Microsoft HoloLens or the VarjoXR-4. These headsets don't require hand controllers to function. Instead, they rely on a variety of sensors and technologies to track and interpret the movements and gestures of the user's hands. Optical sensors are commonly used, which use cameras to capture images or videos of the user's hands. Advanced algorithms then process these images to identify and track the position, orientation, and gestures of the hands in real-time. Other types of sensors can be used for hand tracking and telemetry. Infrared sensors emit and detect infrared light to create a depth map of the environment. This helps in accurately tracking the position and movement of users' hands even in low-light conditions. Leap Motion is a well-known example that uses infrared sensors for hand tracking. Ultrasonic sensors emit ultrasonic waves and measure the time it takes for the waves to bounce back from the user's hands. This data helps in determining the position and movement of the hands. Inertial measurement units combine accelerometers, gyroscopes, and sometimes magnetometers to detect the orientation and motion of the hands. While they are more commonly used in traditional controllers, they can also enhance hand tracking by providing additional movement data. By integrating these sensors, handless controllers in XR environments can offer precise and intuitive interaction, enhancing the immersive experience.

The future of XR technology looks highly promising, fueled by substantial investments from tech giants like Apple, Meta, and Microsoft. These companies are at the forefront of developing next-generation MR devices that aim to offer even more immersive and user-friendly experiences. The introduction of 5G networks and the ongoing miniaturization of processors are expected to further enhance XR capabilities, enabling faster, more seamless interactions.

As AI is increasingly being integrated into XR systems, user capabilities are enhanced. AI algorithms are used to create more realistic virtual environments and interactive elements, improving the immersion and responsiveness of VR and AR applications. For example, AI can enable more natural and intuitive user interactions by recognizing gestures and voice commands, as well as adapting the virtual environment in real-time based on user behavior and preferences. Additionally, AI-driven analytics can provide insights into user engagement and optimize content delivery. This further enhances the overall XR experience, but also raises issues in terms of privacy.

The Apple Vision Pro

To avoid confusion and ensure that all stakeholders were on the same page, CIPPIC used the Apple Vision Pro as a case study during our interviews. We encouraged participants to think about this technology when answering our questions.

Apple released the Vision Pro in the U.S. in early February 2024. It is a headset that creates a three-dimensional user experience through a mix of depth sensors, cameras, microphones and gyroscope.[3] With the launch of the headset, Apple also introduced a brand-new App Store that provides access to more than one million compatible apps and more than six hundred new spatial experiences.[4]

A thorough analysis of the Vision Pro's privacy policies—which isn't a straightforward process, as these documents are scattered on multiple webpages—reveals a concerning issue with respect to the way Apple manages privacy of those who use the headset. Overall, the Vision Pro is designed in a way that should minimize privacy harms, the data is stored on the Vision Pro's hard drive rather than in the cloud, for instance. However, Apple doesn't shoulder much of the responsibility for protecting its users' privacy. The software licence agreement excuses Apple from all liability relating to the content of third-party apps. And this is reiterated in best practices for app developers in which Apple clearly states that: "it's your responsibility to protect any data your app collects and to use it in responsible and privacy-preserving ways".[5]

This may alarm those familiar with Canadian privacy law, as it looks like the arrangement that Facebook had with "thisisyourdigitallife", the app that was responsible for sharing the data of over 600,000 Canadians to Cambridge Analytica. In 2023, the Federal Court found that Facebook couldn't be held liable for the incident under PIPEDA.[6]

---

[3] Apple, "Apple Vision Pro Privacy Overview - Learn how Apple Vision Pro and visionOS protect your data" (2024) at 3, online (pdf).
[4] Apple, "Apple announces more than 600 new apps built for Apple Vision Pro" (1 February 2024), online: *Apple Newsroom.*
[5] Apple, "Adopting best practices for privacy and user preferences", Online: *Apple Developer.*
[6] *Canada (Privacy Commissioner) v Facebook Inc*, 2023 FC 533 at para 65. [*Facebook*]

2. How Does Extended Reality Affect Privacy?

While privacy concerns associated with XR technologies are not unique, the bundling of privacy concerns within XR devices is unprecedented. In other words, while XR doesn't represent a fundamental shift in privacy concerns, it does cause a shift in magnitude. Two main elements characterize this shift.

First, XR headsets process an unprecedented amount of data and the sensitivity of the data is unparalleled. XR headsets have many sensors and captors that collect data in real-time. Those who use the Apple's Vision Pro, for example, must set up sensors that track their eye and head movements.[7] These sensors collect data to provide a more fluid and personalized experience. However, this data can also serve other purposes. Head and hand motions can be used to infer a person's marital status, sexual orientation, or ethnicity, for instance, and the involuntary dilation of a person's pupil can also reveal what they're interested in—or what they're excited about.[8] This offers business opportunities to tech companies. Meta, for example, plans to improve advertisement personalization by tracking eye movements and facial expressions.[9] Several interviewees mentioned this possibility as a source of concern. XR blurs the lines between virtual and actual experiences and is particularly well-suited to influencing consumers.[10]

Second, XR systems are inherently designed to process data about other people—often, without their consent. XR devices are equipped with external cameras and LiDAR that scan the user's surroundings to create a digital map of the user's space. When a person is in the device's field of view, the headset processes data about that person, whether they have consented to it or not. In the case of the Apple's Vision Pro, for instance, the "people awareness" feature actively detects people in the user's environment and displays them on the built-in screen allowing the user to interact with them without having to remove the Vision Pro headset. Given that consent is the cornerstone of Canadian data protection laws, and that bystander-effects are by-products of XR technologies, a number of interviewees highlighted that XR technologies create situations that are not really contemplated under current iterations of Canadian privacy law.

---

[7] Apple, "Redo Eye and Hand Setup on your Apple Vision Pro", online: *Apple Vision Pro User Guide.*
[8] Brittan Heller, "Revisiting Code as Law: Regulation and Extended Reality" (1 September 2023) at 6, online.
[9] Nelson Reed & Katie Joseff, "Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know" (2022) at 1, online (pdf): *Common Place*.
[10] Clifford Nass, BJ Fogg & Youngme Moon, "Can Computers Be Teammates?" (December 1996) 45:6 Intl J Human-Computer Studies 669.

3. Is Canadian Law Well Equipped to Protect XR Users?

The Canadian legal landscape regarding privacy and data protection is a patchwork. Different laws apply whether you are interacting with private corporation or public entities, or if personal health information is processed. While the *Personal Information Protection and Electronic Documents Act* (PIPEDA) theoretically governs how private companies process data nationwide, Alberta, British-Columbia and Quebec have their own laws that supersede it in certain contexts. What's more, PIPEDA itself is multifaceted. The statute is still in force but is on the cusp of being replaced by the *Consumer Privacy Protection Act* (CPPA).

In September 2020, the government tabled Bill C-11, which would have enacted the *Consumer Privacy Protection Act* and the *Personal Information and Data Protection Tribunal Act,* but an election was called and the bill died on the order paper. Then, in November 2022, the Government tabled Bill C-27 to enact the CPPA and the *Personal Information and Data Protection Tribunal Act*. As of May 2024, this bill is at the clause-by-clause consideration stage before the House of Commons Standing Committee on Industry and Technology. However, given the current political context, it is possible that C-27 suffers a similar fate.

This report focuses on the two most relevant pieces of legislation in the context of XR: PIPEDA, and CPPA. They are the most relevant because leading providers of XR technologies like Apple are private companies based abroad and they fall within the scope of the federal regime for the private sector. Both PIPEDA and the CPPA are federal legislation that protect personal information processed by private sector organizations. Like most modern data protection laws, they are rooted in fair information practices, which means that they belong to a family of data protection laws that define privacy partly as one's ability to control how his or her personal information is handled and communicated to others. And thus, like most modern data protection laws, PIPEDA and CPPA both are consent-focused legislations.

Consent is the mainstay of the current federal private sector regime. Except for the processing of data for inappropriate purposes, organizations subjected to PIPEDA can collect, use and share personal information as they want provided they obtain informed consent.[11] Under the CPPA, the principle of consent remains the default rule to legitimize data processing, but its importance is diluted by the introduction of the "legitimate interests" and "business activities" exceptions to consent for processing data. Organizations can collect or use user data without their consent if it is for one of a set of prescribed reasons set out in the legislation. These include an activity necessary to operate the XR device, an activity needed for the organization's information or network security,

[11] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c 5, s 5 [PIPEDA].

the safety of the service or "any other prescribed activity."[12] Under the legitimate interests exception to consent, an organization can process a user's data without their consent if it is for a purpose in which the organization has a "legitimate interest" that outweighs the potential adverse effect on the user.[13] The collection can't be used to influence the user's behaviour under this exception. The CPPA also changes the way consent is interpreted and applied. The new statute would require using plain language in consent forms, for instance. While this looks like an improvement at first, this new obligation is actually less stringent than what PIPEDA requires. The next section analyzes how effective PIPEDA and CPPA are at protecting the privacy of people interacting with XR technologies.

3.1. PIPEDA – The Act that Currently Governs Data Processing in the Private Sector

PIPEDA is outdated and falls short with properly regulating modern digital technologies. The federal court refusal to sanction Facebook for the role it played in the Cambridge Analytica scandal,[14] or to hold Clearview AI accountable for engaging in mass surveillance are examples of PIPEDA's inadequacy.[15] Members of Parliament are working on Canada's second attempt to revamp PIPEDA. As a result, this report will not focus heavily on its flaws. Instead, we briefly present it as a baseline against which we compare CPPA, to determine if the reform truly results in Canadian's privacy being better protected.

According to Chantale Bernier, PIPEDA principles are generally adequate. They are broad enough to apply to XR technologies. Of course, modernizing certain principles to make them more specific about certain technical aspects that have evolved since the law was first passed—like biometrics, for instance—would be warranted. But broadly speaking, the principle is written in a technologically neutral fashion that allows it to remain relevant despite technological changes. To illustrate PIPEDA's applicability to XR, Bernier gives two concrete examples, and highlights some minor changes that would improve the protection PIPEDA offers to Canadians interreacting with XR technologies.

The first example regards the use of VR therapy to treat post-traumatic stress disorder. Under PIPEDA, a company offering this kind of service would be subject to heightened requirements for

---

[12] Bill C-27, *The Consumer Privacy Protection Act,* 1st Sess, 44th Parl. 2022, s 18(2) (first reading 16 June 2022) [CPPA].
[13] *Ibid,* at s 18(3).
[14] *Facebook*, *supra* note 6.
[15] *Doan v Canada (Attorney General)*, 2023 FC 236.

consent and security safeguards because health information is sensitive.[16] Therefore, the consent for processing the data would have to be express, and the measures for ensuring the security of the data would have to be higher than what they would normally be for other kinds of personal information.[17] Moreover, like any other businesses processing data, a VR therapy organization would also have to limit its collection, retention and use of personal information to only what is necessary to accomplish its purposes.[18]

These principles are sufficient to ensure a good-enough protection of Canadians' privacy—as long as companies abide by the rules. And this is often where the problem lies with PIPEDA. It's not necessarily that the substantive rules aren't enough, but rather that these principles are difficult to enforce. To ensure that companies are transparent about the security, retention and use of the data they process, Bernier suggests giving auditing power to the government. She also recommends enshrining the relationship between the sensitivity of the data and the stringency of the legal requirements more clearly into the legislation, so that businesses clearly know their obligations.

The other example Bernier discusses is children using the Vision Pro for entertainment purposes. She's not opposed to the idea that XR companies like Apple process certain personal information about children that uses this technology. However, children have a diminished capacity for meaningful consent so businesses should ask for parental consent to process children's data. This is more or less what PIPEDA already requires. In its guidelines for obtaining meaningful consent, the OPC says that but for exceptional circumstances, children under 13 can't consent to the processing of their data.[19] For minors between 13 and 18, the guidelines states that organizations processing personal information must adapt their consent request to the level of maturity of the users they're interacting with.[20] Moving forward, Bernier says, an updated version of PIPEDA should clarify these requirements and integrate them explicitly into the law.

Given that children are in their formative years, Bernier also suggests that XR companies should avoid storing the information they collect about their young users on their own servers. They shouldn't store more data than what really serves the purpose of the XR system, and they should delete the data as soon as it no longer serves the purposes for which they were collected.

---

16 *Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, being Schedule 1 to PIPIEDA, supra note 11, at ss 4.3, 4.7.
[17] *Ibid,* at ss 4.3.6, 4.7.2.
[18] *Ibid,* at s 4.4.
[19] Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (2021) online: *Office of the Privacy Commissioner of Canada.*
[20] *Ibid.*

Finally, certain kinds of data processing associated with XR that are neither necessary nor proportionate simply shouldn't be allowed for children. While PIPEDA doesn't have any explicit provisions concerning minors, the way it has been applied over the years is coherent with what Bernier proposes. For instance, the Office of the Privacy Commissioner ruled that Nexopia violated PIPEDA because it made its users "visible to all" by default which was inappropriate for a youth-oriented social media.[21] All in all, while PIPEDA already provides for much of what Bernier proposes, certain elements—the age of consent, and the no-go zones—could benefit from clarification.

3.2. CCPA – The Act Proposed to Govern Data Processing in the Private Sector

CPPA is more an updated version of *PIPEDA* than a true overhaul. If the bill passes, consent will remain the backbone of Canada's data protection regime, though with some amendments to facilitate its application and enforcement. Does the bill adequately protect the privacy of Canadians? For many of our interviewees, the answer is no.

During our interviews, several people raised concerns about having a statute that is so heavily focused on consent. For Jane Bailey and Jacquelyn Burkell, consent is ill-equipped to govern XR because information is relational and one's consent has implications for others. As mentioned earlier, XR devices collect data about bystanders who have no real power to object to the collection of their information—they might not even be aware of it. This affects their autonomy and dignity as it deprives them of the ability to control how information about them is collected and shared. Given the fast-paced progress of technologies, and the "sticky" nature of data[22] it has become almost impossible to give a truly informed consent—nobody really knows what the future holds. Bailey illustrates the issue with a striking example: until a few years ago, people posted pictures of their kids without any worries. Nowadays, a "picture of your kid when they were 10 years old can be turned into deep fake porn five years from now, in a world that you didn't even imagine at the time that you posted the image". Consent isn't adequate to capture these new realities.

Valerie Steeves opines that data protection laws and their over reliance on consent are not sufficient. She advocates for a shift towards human rights approaches that are more grounded in the social and democratic values of privacy. She believes that privacy would be better protected with instruments that adopt the language of human rights, as it would provide touchstones for courts to interpret when new situations arise. Thus, she suggests that CPPA should include some clear

---

[21] *Nexopia*, (February 2013) PIPEDA Report of Findings #2012-001, online.
[22] Coined by Wendy Wong. It illustrates that once the data is collected, it's never truly possible to get rid of it. Wendy Wong, *We, the Data, Human Rights in the Digital Age (*Cambridge, Ma: MIT University Press, 2023).

human rights commitments. Leslie Regan Shade offers concrete illustrations of what including clear human rights commitments in CPPA could look like. First, she says, privacy is a human right protected by international human rights law instruments, and it should be recognized as such in both the preamble and the purpose clause of the CPPA.[23] Second, Canada has a duty to incorporate the best interests of the child into legislation and policy under the *Convention on the Rights of the Child*. To comply with its obligation, the government should amend the provision on minors[24] to state that the best interests of the child are a primary consideration for all matters affecting minors.

That would give strength to the rest of the statute. For instance, having a clear reference to the best interests of the child would have an impact on the way courts read the "appropriate purpose clause"[25] of the CPPA. This would constitute a true step forward in comparison to section 5(3) of PIPEDA which can't benefit from a generous and liberal interpretation because PIPEDA's purpose is to strike a balance between commercial interests and the protection of users' rights.[26] Concretely, it would make it easier for the privacy commissioner to rule that certain uses, like using children's data for micro-targeting advertisements, is illegal.

Outright bans of certain kinds of data processing are sometimes called "no-go zones". Almost all our interviewees mentioned that these would be a welcomed addition to CPPA. Whether they suggested this to be done through broad open-textured provisions backed with interpretive principle rooted in human-rights law or a codified list of prohibited kinds of data processing depended, but most of them were in favor of the idea of prohibiting certain kind of uses of XD.

Having "no-go zones" would fit well into the preventive turn that the government is taking with CPPA. Rather than relying solely on litigation and ex-post sanctions, CPPA proposes measures to prevent harm from happening. Mainly, it requires that businesses document the data protection choices they make. For instance, to process personal information without consent under the "appropriate purpose" exception,[27] organizations must record the purpose for which they want the data. To collect information under the "legitimate interest" exceptions,[28] organizations must conduct a privacy impact assessment. The exercise of documenting and keeping track of privacy choices incentivizes organizations to act more responsibly. It also facilitates investigations and

---

[23] CPPA, *supra* note 12 at s 5.
[24] *Ibid,* at at s2(2).
[25] *Ibid,* at s 12.
[26] *Facebook,* supra note 6 at para 50.
[27] CPPA, *supra* note 12 at s 12(1).
[28] *Ibid,* at s 18(3).

sanction for organizations who are careless about privacy. Several interviewees were in favor of this kind of privacy-by-design measures.

According to Chantale Bernier, Privacy Impact Assessments can be very helpful in determining the scope of privacy protections needed for a certain technology and ensuring that the privacy implications do not outweigh the benefits of the technology. Relatedly, Valerie Steeves suggested that researchers develop guidelines providing a clear methodology to help industry think through the human rights implications of the technology they're developing. This echoes something that we also heard in the interviews with industry stakeholders. Indeed, both Caroline Dupuis and Matthew Sherdown noted that they would appreciate having more guidance from the Privacy Commissioner as to how to deal with privacy issues arising from new technologies such as XR.

4. Recommendations - What does CIPPIC Suggest?

The rapid evolution of XR technologies demands a robust framework that protects user privacy, particularly that of vulnerable groups such as children and adolescents. Integrating XR technologies into everyday life presents unique challenges and opportunities for privacy protection. To navigate this complex terrain, this report proposes a comprehensive set of recommendations to strengthen privacy safeguards, enhance regulatory measures, and foster an environment of informed and conscious use of XR technologies. We offer these recommendations to address the multifaceted nature of privacy concerns in XR, from the development phase to everyday use. Our approach protects privacy and upholds the highest standards for Canadian users without stifling innovation in XR technology.

XR technology poses multi-faceted privacy problems and legal regulation alone is unlikely to address them. Instead, CIPPIC recommends a multimodal approach, as described by Lawrence Lessig in his 2006 book, *Code: Version 2.0*.[29] In *Code*, Lessig identifies four types of behavioural regulation in cyberspace: the law, social norms, the market, and technology.[30] These four types of regulation play different roles in cyberspace.

The Law threatens consequences for those who defy it.[31] **Social Norms** threaten community-based sanctions for those who transgress acceptable standards.[32] **The Market** constrains access through pricing structures and economics.[33] **The Technology** limits software and hardware to make certain behaviours possible or impossible.[34]

No single regulatory approach can fully address the privacy issues posed by XR technologies. Instead, approaches that address all four behavioural regulators, leaning heavily on social norms and legal approaches, are necessary.[35] Education and empowerment can influence how people view individual privacy and acceptable data collection, creating social norms that support stronger regulation. Users looking to purchase XR technology should be aware of what apps and devices best uphold their privacy rights so they can choose the business that best caters to their expectations concerning privacy. While Apple has already begun incorporating technological limits on XR

---

[29] Lawrence Lessig, *Code: Version 2.0,* 2nd ed (New York: Basic Books, 2006) at 123; see also Brittan Heller, *supra* note 8.
[30] *Ibid* at 123.
[31] *Ibid* at 124.
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid* at 125.
[35] *Ibid*; see also Heller, *supra* note 8.

devices' capabilities with its Vision Pro, stricter guidelines must be implemented and more widely accepted to affect the marketplace.

4.1. The Law - Adopt a Purposive Reading of PIPEDA and Amend the CPPA

It is clear that XR requires stronger regulation. CIPPIC proposes three potential direct legal approaches to addressing XR technology's involvement in the collection, use and sharing of personal information: (1) interpreting the current law's requirement for meaningful consent to involve active, informed versions of opt-in consent; (2) convening a consultation for the development of a co-regulatory guideline document that will inform the enforcement of the current law; or (3) amending the proposed Bill C-27 to take into account the specific challenges of XR technologies.

(1) *PIPEDA* Interpretation: The OPC could interpret PIPEDA to require explicit consent with a detailed explanation of the platform's intended use of the data. PIPEDA is a consent-based framework. Under this model, organizations must obtain meaningful consent from users to collect, use, and disclose their personal information. XR devices accrue large volumes of user data, their environment, and third-party bystanders to function at a basic level. Given the magnitude and types of data collected by XR technology, obtaining meaningful consent is impossible under PIPEDA's current interpretation. However, as Chantal Bernier stated, PIPEDA is a principled-based law that can be interpreted in context. XR technologies gather time-sensitive information, either inherently (children, biometric, etc.) or by virtue of its unexpected context (bystander effect). The OPC could, through an Interpretation Bulletin, signal that the Commissioner intends to interpret PIPEDA to require explicit, opt-in consent in the presence of detailed explanation of the platform's intent, and within contexts that allow a considered assessment of that intent (and not, for example, during gameplay). This approach would effectively eliminate the collection of information about bystanders since it is impossible to obtain meaningful consent from them. This would also require considered approaches to engaging children, since it is impossible to obtain meaningful consent from a child.

(2) Co-regulatory Guidelines: Under the current law, the OPC could adopt what is in effect a "co-regulatory" model. The OPC could convene a consultation among stakeholders in the XR technology space to find consensus about the law's current requirements of commercial actors in this context. The OPC could then use this consultation to prepare interpretational guidance that would instruct XR technology makers and app developers on how the Commissioner intends to enforce PIPEDA. This approach could address many of the legal privacy issues identified.

(3) Bill C-27 Amendments: Privacy issues with XR technologies could also be addressed through amending the proposed Bill C-27, the CPPA. Broadly, the similar recommendations in its submission to Parliament regarding Bill C-27.

The CPPA should define "sensitive information" to include information for which an individual has a heightened expectation of privacy or if its disclosure risks harm to the individual. This may include health, biometric and genetic data, along with minors' personal information. By doing this, it covers the wide breadth of information XR devices collect about users. This should be coupled with substantive safeguards to ensure organizations consider the privacy risks inherent with collecting and using such information.[36]

Amendments to the CPPA should also include putting individuals at the centre of consent and its exceptions. This could be done by ensuring user consent is meaningful by legislating a requirement to make sure it is reasonable that users directly understand what they are being asked. It is worth noting that PIPEDA provided for such a standard in s.6.1, but the CPPA appears to apply a less stringent standard in s.15(4), which only mandates the organization provide the information in "plain language" that the individual would reasonably be expected to understand. It could also be done by removing the ability to imply consent and increasing transparency around exceptions to consent. This would address issues around the heightened concern over data collecting and data sharing with XR technologies.

Thirdly, some privacy concerns around XR can also be addressed by strengthening the protections for children's privacy in the CPPA. The best interest of the child should be the primary concern for companies providing online services to children. This could be reflected in the definition section of the legislation. Additionally, there should be a requirement that privacy settings be "high" by default for children. This would specifically address their vulnerability and safeguard against the collection, use, and disclosure of their biometric data. The CPPA has not been enacted

[36] The House of Commons INDU committee appears to have passed a similar amendment during its clause-by-clause review of the legislation at its May 22 meeting. This is a positive development as the definition includes information about an individual that reveals core characteristics, such as race, political opinions, sexual orientation, genetic data, government identifiers, etc. The definition includes information on individuals' health conditions and any treatment or prescriptions they are receiving. -- House of Commons, Standing Committee on Industry and Technology, *Evidence,* 44-1, No 124 (22 May 2024) at 16:03 (Joël Lightbound)

as of the time of writing. The opportunity is prime to make consequential amendments that will address privacy concerns around emerging XR technologies and protect Canadians' data.

4.2. Social Norms - More Privacy Education Needed

Privacy education is key to regulating privacy in XR spaces. The OPC can assist by preparing educational materials focused on users, but also XR technology makers and app developers, something the private industry stakeholders said would be helpful during interviews with CIPPIC.

Users are often casual when it comes to privacy with XR platforms. Dedicated OPC materials educating users about their right to privacy in XR and the steps they can take to limit intrusions from XR companies can help address this concern. Separate materials for adults and children and their inability to provide meaningful consent would be especially useful. The Institution of Engineering and Technology estimates that among parents whose children already interact with VR, more than 25% do not know what kind of worlds their children are on, and more than 60% do not understand anything about the metaverse.[37] However, even mature users need more dedicated, trusted resources, and the OPC is best equipped to provide them.

Commercial actors also require privacy education and the burden should not fall completely on users. The OPC can provide this educational guidance in the form of Interpretational Bulletins, Guidance documents, and Fact Sheets, as well as public engagement in the media, at conferences, and before lawmakers. OPC educational initiatives can influence both the design and deployment of XR technologies.

Finally, enforcing PIPEDA itself against offenders has a powerful influence on social norms and behaviours in the marketplace. Under PIPEDA, the Privacy Commissioner is both an ombudsperson, promoting compliance with the law, and an enforcer, investigating and pronouncing on violations, and bringing them to court for enforcement. Enforcement can be an effective tool to promote compliance and change norms. When society at large sees the OPC taking action against PIPEDA offenders and real consequences for violations they are more likely to follow the law and comply with the legislation. This creates a new social norm where those in the market are more likely to protect user privacy as they see failures to results in consequences.

[37] The Institution of Engineering and Technology, Press Release, "Generation VR" (19 April 2022) online.

4.3. The Market – Introduce a Privacy Grading System

The OPC could consider introducing a grading system for XR devices and apps. This would be a way for users to decide how to spend their money. XR users currently do not have any standard to follow and there is a wide variety of choice in the market. The Office of the Privacy Commissioner currently publishes Guidelines on numerous privacy technologies but does not assess marketplace competitors with compliance with those guidelines. Doing so would give greater power to such documents, promote competition over privacy, and make it easier for consumers to exercise privacy power in the market. Similar programs already exist in other industries. For example, the Environmental Working Group has its own rating system for how "clean" a beauty product is to help users identify issues such as cancerous materials, allergens, and various toxicities.[38] Under this system, users who prioritize clean beauty can invest their money in products that align with some standard. Some corporations in XR are more privacy-oriented than others. Apple's Vision Pro, for example, stores as much data as possible on its user's device without sharing it with third parties. Meta, in contrast, stores user data on the Oculus' cloud backup, arguably a less privacy-friendly approach to data storage since the user has less control over the data and it is more vulnerable to breach. A privacy grading system can help consumers quickly decide which product is best for them. Ultimately if individuals purchase products from XR companies with higher privacy standards, other companies in the market may adopt a higher privacy standard in response.

4.4. The Technology – Promote Privacy by Design

Technology functions as a regulator by allowing or denying certain behaviours through the capabilities of the technology itself. While the OPC is not a technology developer, it can influence how technology develops and how companies deploy it through developing best practices documents, guidance documents, and Interpretation Bulletins. For example, guidance requiring the adoption of privacy by design rules in technology development and deployment could help address privacy concerns at the level of the device itself. Identifying privacy standards the Canadian marketplace should adopt could also encourage the adoption of more privacy-friendly technology. XR companies are in a unique position to address users' privacy concerns. While XR programs require certain data to run, companies can control who has access to that data and how it is stored. They can control the circumstances in which a user encounters requests for the collection, use and sharing of data. For example, Apple already has built-in limits on third-party access to user data with its Vision Pro but can further improve its privacy standards, especially regarding children-oriented games. Because of the unique concerns that arise with children, Apple

[38] The Environmental Working Group, "Understanding Skin Deep® Ratings", online: *EWG's Skin Deep.*

could implement a specific parental control mechanism to let parents control the games their children can download on the device and limit the data third parties can request in-game.

The OPC could also consider adopting a comply-or-explain enforcement model, requiring companies to justify why they are not adhering to a privacy standard. The model could be similar to the Securities Commissioner's, which requires companies to either comply with the commissioner's diversity disclosure standards, or explain their adherence failures and risk enforcement action.[39]

[39] Andrew Pollock, "Canadian Securities Administrators Propose Enhanced Diversity Disclosure", Norton Rose Fulbright (19 April 2023).

Conclusions

The development and deployment of XR technologies presents unique privacy challenges, but also offers an opportunity to develop an innovative regulatory framework that addresses current privacy challenges while accommodating technological innovation. This kind of framework necessitates a dialogue between policymakers, industry leaders, privacy advocates, and consumers to ensure that a commitment to privacy, ethical considerations, and respect for individual autonomy guides the regulatory hand.

With XR technologies crossing international borders, Canada could provide a framework for privacy protection that other jurisdictions could replicate. Education and awareness are also key components of our proposed approach. Canada can cultivate a more privacy-conscious society by informing the public about XR technologies' privacy implications and equipping individuals with the tools to navigate this new digital terrain. This includes developing resources for parents and educators to protect children's privacy in XR environments. Investing in research and development to explore privacy-enhancing technologies and methods for XR is another pivotal step. This strategic move could pave the way for innovations that enable more secure and privacy-respecting ways to take advantage of XR without compromising personal data. A comprehensive privacy framework for XR technologies requires proactive legislation, robust public-private engagement, public education, and ongoing innovation.

Appendix

Interview with stakeholders – Recruitment Process

CIPPIC contacted several Canadian academic researchers whose work focused on user data privacy in preparation for this study. CIPPIC also contacted Chantal Bernier, former Privacy Commissioner of Canada and current counsel in Privacy and Security at Denton's,[40] because of her extensive expertise in privacy and cybersecurity matters in both the public and private sectors. A summary of all participants' professional expertise can be found in Appendix 1 at page **Error! Bookmark not defined.** below. Any new stakeholders these selected interviewees mentioned were added to the interview collection pool if their colleagues believed they could bring relevant expertise to this project. As a result, CIPPIC contacted two additional academic researchers whose work focuses on the technical aspects of XR technologies (ethics and engineering; privacy-enhancing technologies). Unfortunately, attempts to schedule interviews with these additional individuals were unsuccessful.

The interviewee pool also included technical, legal, and public policy staff at companies making XR technologies. Ten professionals were contacted via email or LinkedIn. Out of the ten professionals contacted, three responded and were interviewed simultaneously.

Finally, CIPPIC contacted four organizations dedicated to children's safety on the internet. CIPPIC chose these organizations because they had published materials specifically related to children's safety when using XR technologies. Of these four organizations, one responded. The organization committed to an initial meeting to discuss the focus and goals of the project, but their organizational priorities would not permit them to respond to questions before this report's deadline.

CIPPIC contacted stakeholders and informed them that the Office of the Privacy Commissioner of Canada had awarded CIPPIC a grant to study the personal privacy ramifications of data collection within XR technologies, with a particular emphasis on children's privacy. CIPPIC informed stakeholders that limited studies existed evaluating the relevance or sufficiency of privacy laws governing XR, and no studies had approached this issue from a Canadian viewpoint. CIPPIC also notified stakeholders that CIPPIC would consider potential shortcomings in prevailing or proposed laws and to identify potential legal safeguards. CIPPIC informed stakeholders that Apple's Vision Pro headset was the primary case study for CIPPIC's research.

[40] For more information, see Chantal Bernier's biography published by the University of Ottawa.

CIPPIC selected stakeholders to participate in CIPPIC's research because the literature identified them as a diverse set of Canadian legal specialists, app developers, and others who could provide a comprehensive understanding of the privacy implications of XR technologies. Stakeholders were told that the insights gathered from their interviews would play a pivotal role in shaping CIPPIC's analysis, ensuring CIPPIC could provide a comprehensive opinion on privacy considerations associated with XR technologies. Stakeholders were informed that the culmination of CIPPIC's research would be presented to the Office of the Privacy Commissioner of Canada, policymakers, scholars, and the public prior to participation. They were also told that CIPPIC's research team would be conducting all interviews via videoconference and that the interview would last approximately one hour.

When stakeholders agreed to participate, they received videoconference meeting details and a document with details about CIPPIC, a summary of the project's topic and goals, how their answers would be used, and questions they could expect to answer during the interview.

Interview with stakeholders – Participants' Bio

Academic Stakeholders

All four of these academic stakeholders are involved with the Social Sciences and Humanities Research Council's eQuality Project. Professor Steeves and Professor Bailey co-lead the organization, and Professor Shade and Professor Burkell are investigators. The Project "is dedicated to the creation of new knowledge about young people's use of networked spaces, with special emphasis of privacy and equality issues."[41]

Professor Jacquie Burkell is the Associate Vice-President of Research at the Rotman Institute of Philosophy and an Associate Professor in the Faculty of Information & Media Studies at Western University. Her research broadly focuses on the social impact of technology and examines how technological mediation changes social interaction and information behaviour.

Professor Leslie Regan Shade is a Professor in the Faculty of Information at the University of Toronto. Since the mid-1990s, her research focus has been on the social and policy aspects of information and communication technologies, with particular emphasis on issues of gender, youth and political economy. She is a recipient of the SSHRC Insight Grant on the relationship between young adults and digital privacy.

[41] The eQuality Project, "Research Projects."

Professor Jane Bailey is a faculty member at the University of Ottawa Centre for Law, Technology and Society and a Full Professor of Law within the Faculty of Law, Common Law Section. Her research focuses on the societal and cultural implications of emerging private technological controls, particularly concerning members of socially disadvantaged communities. Her research also focuses on harassment, hate, privacy, and equality concerns arising from online behavioural targeting of youth.

Professor Valerie Steeves is a faculty member of the Centre for Law, Technology and Society and a Full Professor in the Department of Criminology of the Faculty of Social Sciences at the University of Ottawa. Her research focuses on new technologies' impact on human rights. She has been an expert witness before Parliamentary Committees regarding privacy legislation and developed privacy education curricula for government departments. She is the lead researcher for MediaSmart's Young Canadians in a Wired World research project.

Private Industry Stakeholder Participants

Chantal Bernier dedicated nearly six years to being at the helm of the Office of the Privacy Commissioner of Canada. During her time with the OPC, she lead national and international privacy investigations in the public and private sectors, privacy audits, privacy impact assessment reviews, technological analysis, and privacy policy development and research. She is now the co-chair of the Global Privacy and Cybersecurity Group at Dentons, where she advises leading-edge national and international companies as they expand into Canada and Europe, enter the e-commerce space, adopt data analytics and roll out data-based market initiatives. Her clients include ad tech companies, financial institutions, biotech companies, data analytics firms and government institutions.

Caroline Dupuis is the Learning Network's Senior Vice President of XR Products. Her specialties include understanding the software development lifecycle framework and establishing strong stakeholder relationships. Previously, she worked at ICOM Productions as an AR/VR Project Manager, working with instructional designers, artists, and content developers to create and execute client specifications for XR technologies.

Matthew Sheardown is the Learning Network's Learning Design manager of XR Products. He oversees and manages the learning design and development of XR and 3D projects for clients on various XR platforms. He previously worked as a Lead Designer of XR Products at ICOM Productions, directing instructional design and learning principles for all XR projects.

Alex Gimson is a Game Developer and XR Project Lead at ICOM Productions. He holds a bachelor's degree in New Media from The University of Lethbridge. He has worked in the XR industry for almost four years and has been doing development work for over a decade. His most recent development work is Ocnus Theory, a 3D sandbox platformer that tests creative problem solving by picking up blocks to climb a very tall tower after a painful fall.

Interview with Stakeholders – Questionnaire

XR technology's impact on privacy:

1. Do you think XR technologies can impact peoples' privacy?
2. Do you think people across different demographics are impacted equally?
3. Do you think these privacy concerns are unique to XR technologies? If so, how do they differ? Please explain.
4. How could these privacy concerns be better addressed?

Risks of biometric data collection:

5. Biometric data is the collection of information about people's physical or behavioural characteristics. In your opinion, what are advantages and disadvantages to biometric data collection through XR technologies?
6. Do you think this biometric data collection is ethical? If not, what are your concerns?

Implications of AI on XR technology:

7. How does the potential addition of generative AI to XR technologies change, or have the potential to change, the scope and nature of these privacy concerns?
8. Do you think corporations should be allowed to analyze the data collected from XR technologies with AI?
9. Data anonymization enhances privacy protections for users by removing identifiers that connect the stored data to the user. Do you think integrating AI can increase the risk that users could be identified outside the XR environment?

Adequacy of Canadian privacy law for XR technology:

10. How could privacy protections be better incorporated into the development process for XR technologies?
11. Do you think the existing legal and policy frameworks, such as the *Personal Information Protection and Electronic Documents Act* and the proposed *Consumer Privacy Protection Act* (part of Bill C-27), adequately address the privacy concerns of XR? Are new statutes or regulations required?
12. What is the best forum for consumers to raise their privacy concerns or issues related to XR technologies?

Children's privacy in XR:

13. Are privacy concerns different for adults and children?
14. Do you think storing children's data requires different security protocols? Can you explain?
15. Could AI expose children to an increased risk of manipulation or undermine their agency?