the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

CANADA

Regional Coordinator:
Alejandro Luna *Fandiño Olivares, Ciudad de México*

Data

James Buchan *Gowling, Toronto, Ontario*
Chris Oates *Gowling, Toronto, Ontario*

Q 1. Are there any data (personal and non-personal) policies, strategies or regulations applicable to the metaverse in your jurisdiction?

There are no specific data protection policies or regulations in Canada explicitly tailored for the metaverse. The primary data protection legislation is the federal Personal Information Protection and Electronic Documents Act (PIPEDA), which applies to the collection, use and disclosure of personal information by private sector organisations. The provinces of British Columbia, Alberta and Québec have provincial privacy legislation which applies to the private sector within these provinces. This chapter focuses on PIPEDA, unless otherwise stated.

The Office of the Privacy Commissioner of Canada (OPC) is responsible for enforcing PIPEDA. The OPC provides guidance, investigates complaints and works to ensure that organisations handling personal information comply with the principles outlined in PIPEDA.

Q 2. How are the various personal and non-personal data associated with the metaverse protected in your jurisdiction?

While PIPEDA provides a comprehensive framework for privacy protection, its application to emerging technologies, such as the metaverse, depends on how personal information is handled in these virtual environments. 'Personal information' is broadly defined as 'information about an identifiable individual'. Key to the definition is that the person must be identifiable, not identified. Where the information makes it possible to identify to an individual, including through a combination with other datasets, the OPC will be likely to treat the information as personal information.

PIPEDA sets out the rules for how private sector organisations must handle personal information, including when such data is collected within virtual environments like the metaverse. Some key aspects of how personal information may be protected in the context of the metaverse in Canada, include the following:

- consent – PIPEDA requires organisations to obtain informed consent of individuals before collecting, using or disclosing their personal information. This principle applies to the collection of data within the metaverse, which may include user information, device data and any other associated information;
- purpose limitation – organisations must clearly state the purpose(s) for which they are collecting personal information and must not use or disclose it for purposes other than those for which it was collected, except with the consent of the individual or as required by law;
- limiting collection, use and disclosure – organisations may only collect the personal information needed for their disclosed purposes (data minimisation). Collected personal information may only be used for those disclosed purposes (unless further consent is secured or there is a legal obligation). Consent to process personal information may not be required as a condition of service, unless the processing is truly necessary for the services;
- security safeguards – organisations are required to implement security safeguards to protect personal information against loss, theft, unauthorised access, disclosure, copying, use or modification. Such safeguards must be appropriate for the sensitivity of the information;
- access and correction – subject to exceptions set out in the statutes, individuals have the right to access their personal information held by organisations and request corrections, if necessary. This principle extends to personal information collected within virtual environments;

- accountability and openness – organisations must be accountable for the protection of personal information in their possession and must be open about their privacy practices;
- data retention – personal information may only be retained for as long as needed for the disclosed purposes. Organisations must establish guidelines and practices for retaining personal information only for as long as necessary to fulfil the purposes for which it was collected; and
- third-party relationships – organisations are responsible for the personal information that they transfer to third parties for processing. They must use contractual or other means to ensure that third parties provide a comparable and appropriate level of protection to the information being transferred for processing.

Q 3. Who are the different stakeholders involved in the data value chains on the metaverse and, in the case of personal data, what are their data protection roles? How are their activities regulated under regional/national policies, strategies or regulations?

Stakeholders in data value chains within the metaverse can include platform operators, developers, users, third-party service providers and regulatory bodies. In the context of personal data, their roles and data protection responsibilities are outlined as follows:

- platform operators (eg, metaverse platforms, virtual reality platforms) – platform operators create and manage the virtual environment by facilitating user interactions and transactions within the metaverse. Their data protection role includes collecting and storing user data (avatars, preferences, behaviours) in accordance with privacy laws, implementing security measures to protect user data, providing transparency on data collection practices and obtaining user consent for data processing;
- developers and content creators – developers create virtual worlds, applications and content within the metaverse. They must ensure that applications and content comply with data protection regulations, such that they minimise data collection to what is necessary for the application's functionality, integrate privacy features within applications and collaborate with platform operators to implement privacy measures;
- users – users engage with the metaverse, create avatars and generate or provide personal data through their activities. Users should understand and manage their privacy settings, provide informed consent for data processing, exercise their rights to access and control their personal data. Users may also report privacy concerns to platform operators, other entities involved in the data processing or, potentially, regulators;
- third-party service providers – external entities providing services within the metaverse, such as payment processors, advertising networks or analytics services must comply with data protection regulations, limit data access to what is necessary for the provision of services, and collaborate with platform operators and developers on privacy considerations; and
- regulatory bodies (eg, the OPC and provincial privacy commissioners) – the OPC oversees and enforces PIPEDA, while the provincial commissioners in British Columbia, Alberta and Québec enforce the local laws in their province. In this capacity, the OPC establishes and enforces privacy regulations, investigates complaints related to data protection, issues public findings and rulings, as well as provides guidance on compliance with privacy laws.

Q 4. In relation to personal data, what are the data protection principles (eg, transparency) applicable on the metaverse? What are the most common types of infringement of data protection principles in the metaverse (eg, data minimisation) in your jurisdiction?

Data protection principles in Canada are generally governed by PIPEDA. The key principles include:

- consent – all organisations must obtain the individual's consent for the collection, use or disclosure of personal information, except where not required under the law (note that the exceptions are narrow and specified by the statutes);
- purpose limitation – personal information can only be collected for specific, explicit and legitimate purposes. It cannot be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law;
- transparency – organisations must be transparent about their privacy practices by providing individuals with information about how their personal information is collected, used and disclosed;
- security safeguards – organisations are required to protect personal information through security safeguards against loss, theft, unauthorised access, disclosure, copying, use or modification, as appropriate to the sensitivity of the information;
- accuracy – organisations must make reasonable efforts to ensure that personal information is as accurate, complete and up-to-date, as needed for the purposes for which the information is being processed;
- access and correction – individuals have the right to access their personal information held by organisations and request corrections, if necessary; and
- accountability – organisations are accountable for the protection of personal information in their possession. This includes ensuring that third parties, with whom they share data, provide a comparable and adequate level of protection.

Sanctions for non-compliance with the data protection principles under PIPEDA in Canada can include civil remedies pursued by individuals seeking damages for actual harm suffered as a result of a privacy breach, along with orders by the Privacy Commissioner of Canada to ensure compliance with PIPEDA. Such non-compliance can also potentially result in criminal sanctions, as PIPEDA includes provisions for offences such as knowingly destroying, altering, or falsifying records or obstructing the Privacy Commissioner's investigations. The provincial commissioners may also order and issue binding orders. Recent legislative changes in the province of Québec have introduced much higher penalties in that province, including fines of up to the greater of CAD 10m (approx US$7.28m) or two per cent of worldwide turnover for the preceding fiscal year, increasing for certain offences.

Legislative amendments have been proposed to introduce administrative monetary penalties for non-compliance with a proposed successor to PIPEDA; however, these amendments are pending before Parliament (Bill C-27).

Q 5. In relation to non-personal data, how is data sharing/licensing regulated in your jurisdiction? Is data ownership recognised? How is proprietary information, including any rights to datasets regulated in your jurisdiction? What are the most common types of infringement of these rules in the metaverse (eg, unlawful use of proprietary information) in your jurisdiction?

Canada primarily relies on a combination of intellectual property law, contract law and general legal principles to regulate data sharing, licensing and proprietary information. However, specific regulations addressing non-personal data and data ownership are not as developed as those pertaining to personal data.

Intellectual property law in the Canadian regime recognises intellectual property rights, such as copyright and patent law, which may apply to certain types of non-personal data. Copyright protection may extend to original datasets, while patent law may apply to inventions or innovative methods related to data processing.

Well-established principles of contract law often govern data sharing and licensing agreements. Parties involved can define the terms, conditions and restrictions related to the use and sharing of data. For personal information, such terms would need to comply with the requirements of the privacy laws.

Proprietary information, including trade secrets and confidential business information, is protected under the common law in Canada. Unlike the US, Canada does have a specific legislative framework (eg, statute) governing trade secrets, but well-established legal principles at common law recognise the importance of protecting confidential information.

Common types of infringements relating to the unlawful use of proprietary information include unauthorised access to or use of proprietary information, trade secrets or confidential datasets without proper authorisation or consent, and breach of contract for violations of the terms outlined in data sharing or licensing agreements, such as unauthorised distribution or use of data beyond the agreed scope.

Sanctions for infringements relating to non-personal data may include civil remedies damages resulting from the unlawful use of proprietary information or breach of contract, including injunctive relief and damages for breach of contract. Criminal sanctions may also arise in cases involving unauthorised access to computer systems or unauthorised use of proprietary information.

The most common types of risks of infringement or breaches of the PIPEDA associated with the metaverse (or other digital environments) relate to the following: (1) insufficient consent through collecting or using personal information without obtaining proper consent from users; (2) excessive data collection by collecting more personal information than necessary for the intended purpose; (3) inadequate security measures by failing to implement sufficient security measures to protect personal information from unauthorised access or breaches; and (4) a lack of transparency by not providing clear information to users about how their personal data is being collected, used or disclosed.

Q 6. Are there any policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?

There are no specific policies or regulations applicable to digital marketing in the metaverse in Canada. However, existing laws and regulations that govern digital marketing and consumer protection in online environments, as well as privacy law, will apply to activities in the metaverse. Some relevant legislative considerations include:

- the Competition Act – which includes prohibitions relating to false advertising and deceptive marketing practices. These rules are applicable to digital marketing activities, including those within the metaverse;
- the Canadian Anti-Spam Legislation (CASL) – which regulates electronic messaging, including email, text messages and other forms of digital communication. It sets out requirements for obtaining consent, providing identification information and including an 'unsubscribe' mechanism in electronic messages. Depending on the nature of the message and platform through which it is sent, such requirements could apply to messages sent via a metaverse; and
- privacy laws – PIPEDA and provincial privacy laws in some provinces, apply to the collection, use and disclosure of personal information, including data collected through digital marketing efforts. Ensuring compliance with privacy principles is crucial.

Sanctions for infringements relating to digital marketing in the metaverse may include civil remedies (such as class action lawsuits) for damages or regulatory penalties (such as those from the Competition Bureau that may impose administrative penalties or compliance orders, or the OPC, which may investigate, issue public findings and potentially escalate matters to the Federal Court for a binding compliance order, or award of damages) and criminal sanctions for certain deceptive marketing practices or fraud that may lead to criminal charges under the Competition Act.

- To date, there have not been any specific judicial or regulatory decisions directly related to digital marketing in the metaverse. However, regulatory bodies, such as the Competition Bureau and the OPC, regularly investigate and address complaints related to deceptive marketing, false advertising and privacy violations.

Q 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring protection of minors' data? What is the age of consent for data protection purposes? Is it necessary to verify the consent provided by a responsible adult?

The protection of minors' data is also addressed under PIPEDA and provincial privacy law. PIPEDA does not specify a distinct age of consent for data protection purposes. Instead, it is generally understood that the age of consent for privacy law purposes is determined by the ability of the individual to understand and exercise their rights, that is, their 'capacity'. Minors will have diminished capacity, and for children under 13, case law has held that specific parental consent is required. Under the Québec privacy law (Law 25 or the Privacy Legislation Modernization Act) that age is set at 14 and there is also a ban on targeting advertising to persons under 13. Lastly, in most provinces and territories the age of majority is 18 years old. Note that a minor would not be able to enter a binding contract (a matter distinct from privacy consent, but relevant for eg, terms of use).

Key considerations related to the protection of minors' data under PIPEDA include:

- consent – organisations are required to obtain meaningful consent before collecting, using or disclosing personal information, including that of minors. The consent process should be appropriate for the age and maturity of the child;
- parental consent – for children under the age of majority, organisations often seek parental or guardian consent before collecting personal information. The responsibility to obtain consent from a minor's parent or guardian typically falls on the organisation collecting the data. For persons under 13 (14 in Québec), such specific parental consent would be required. For 'mature minors' the matter is more nuanced, as such persons may have greater capacity to act directly;
- verification of consent – organisations may be required to take reasonable steps to verify that the person providing consent, on behalf of a minor, is authorised to do so; and
- age verification – while PIPEDA does not specify a particular age for consent, organisations may implement age verification measures to ensure compliance with the relevant provincial or territorial laws and to tailor consent processes based on the age of the individual.

Q 8. How are international data transfers regulated in your jurisdiction? Is there any case law or are there any decision by a regulator regarding infringements of these rules in your jurisdiction?

Canada does not have a comprehensive set of regulations specifically governing international data transfers. Instead, the regulation of international data transfers in Canada is generally embedded in the broader framework of PIPEDA and applicable privacy laws. Under PIPEDA, organisations are not only required to protect personal information, but must also safeguard personal information when transferring personal data across borders. The key principles regarding international data transfers, as detailed in PIPEDA, include:

- consent and openness – organisations are required to obtain an individual's knowledge and consent before collecting and processing personal information. Individuals must be informed about the purposes for such processing and the potential risks associated with it. This includes disclosing the risk of foreign 'lawful access' requests for information transferred outside of Canada;
- openness – organisations are required to be open and transparent about their privacy practices and policies. The OPC has held that such transparency includes clear disclosure of the occurrence of international data transfers and the resultant potential for foreign 'lawful access' requests; and
- safeguards – organisations must use contractual or other means to provide a comparable level of protection for personal information that is transferred to third parties outside of Canada. This is to ensure that the information remains adequately protected. While PIPEDA provides these principles, there is no specific certification or approval process for international data transfers, and the responsibility for compliance lies with the organisations handling the personal information.

As for case law or decisions by a regulator specifically related to infringements of international data transfer rules in Canada, specific instances may be less common compared to cases involving other aspects of privacy and data protection. However, the OPC is the regulatory body responsible for overseeing compliance with PIPEDA and it has issued guidance on international data transfers. The OPC may investigate complaints related to the handling of personal information, including international data transfers. For personal information subject to the Québec privacy law, a specific form of privacy impact assessment is required before transferring personal information outside of Québec, which includes assessment of the data protection laws and principles in place in the destination jurisdiction, among other things.

Q 9. How is automated decision-making regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of these rules in your jurisdiction?

Canada has not yet implemented specific regulations solely dedicated to automated decision-making. However, automated decision-making is subject to the general principles and requirements outlined in PIPEDA (while not being explicitly outlined in the legislation). Key principles relevant to automated decision-making under PIPEDA include consent, purpose limitation and accuracy, as well as the right of individuals to have access to their personal information held by organisations and to be able to make corrections, if necessary. These principles also extend to information used in automated decision-making.

The privacy law in the province of Québec does include increased transparency obligations in respect of automated decision-making, and this area would also be subject to more specific regulation should Bill C-27 be adopted federally.

Q 10. What rights are granted to individuals for protecting their rights on the metaverse and how can they exercise them? What is the level of enforcement based on private claims in your jurisdiction?

Generally speaking, the rights of individuals in the metaverse in Canada are primarily governed by the existing privacy laws and other laws. In the absence of specific metaverse-related regulations, individuals have certain rights related to the protection of their personal information and consumer rights that apply both in the metaverse and more broadly. The primary legislation relevant to these rights is PIPEDA.

Rights granted to individuals for protecting their privacy and exercising control over their personal information in the metaverse include:

- the right to consent – individuals have the right to provide informed consent before their personal information is collected, used or disclosed in the metaverse;
- access and correction – individuals can request access to their personal information held by organisations in the metaverse and request corrections if necessary;
- privacy settings and controls – platforms operating in the metaverse should provide users with privacy settings and controls to manage the visibility and use of their personal information, along with the ability to exercise any available choices as to how it is processed (noting the data minimisation and limitation of use principles discussed above);
- security safeguards – individuals have the right to expect that their personal information will be protected through reasonable security measures in the metaverse; and
- complaints to regulatory authorities – individuals can file complaints with the OPC, if they believe their privacy rights have been violated in the metaverse.

Enforcement of private claims in Canada are typically filed with the OPC. The OPC has the authority to investigate complaints, issue findings and make recommendations. However, the enforcement level based on private claims can depend on various factors, including the nature and extent of the alleged violation. The OPC does not have the authority to award damages to individuals. Rather, individuals (or conceivably the OPC) must pursue legal action through the courts

to seek remedies, such as damages for privacy violations. Private claims may be filed in civil courts and the outcomes can vary based on the specific circumstances of each case. At the same time, the provincial commissioners have a greater power to issue binding enforcement orders than the OPC. The province of Québec has introduced high penalties in the province, including fines of up to the greater of CAD 10m (approx US$7.28m) or two per cent of worldwide turnover for the preceding fiscal year, increasing for certain offences.

Q 11. Are there any upcoming policies, strategies or regulations that will impact the use of data on the metaverse?

Legislative amendments have been proposed in Canada to introduce administrative monetary penalties for non-compliance through a proposed successor to PIPEDA; however, these amendments are pending before Parliament (Bill C-27).

Cybersecurity and the metaverse

Elisa Henry *Henry Tech, The Hague*
Anais Galpin *Harmony Energy France, Montreal, Quebec*

Q 1. Are there any cybersecurity policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Specific cybersecurity policies, strategies or regulations directly addressing the metaverse in Canada have not been explicitly established. However, the country's privacy and cybersecurity requirements are technology neutral and are, therefore, generally applicable to digital environments and, as such, would apply to the metaverse.

Canada's Digital Charter

In June 2018, Innovation, Science and Economic Development Canada (the federal ministry in charge of innovation or ISED), initiated national digital and data consultations with many stakeholders (including business owners, researchers and innovators) on the challenges and opportunities in the current digital technology landscape.

In 2019, following these consultations, the ISED published its National Digital Charter, which provides ten principles, described by the ISED as 'the foundation for a made in Canada digital approach that will guide [its] policy thinking and actions and will help to build an innovative, people-centred and inclusive digital and data economy'.[1] The principles include themes related to cybersecurity and privacy, such as safety and security, control and consent, transparency, portability and interoperability, strong enforcement and real accountability.

The unveiling of the National Digital Charter led the Canadian government to seek a reform to the current federal legislation on privacy, after a discussion paper was issued containing proposals to modernise PIPEDA. A bill, the Digital Charter Implementation Act 2022,[2] was introduced in the House of Commons on 16 June 2022, which aims to create three new federal laws: the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (Tribunal Act) and the Artificial Intelligence and Data Act (AI Act). Details on the major changes proposed by this new set of legislative rules and their possible effects in terms of cybersecurity requirements, which are still currently being considered by the House of Commons, will be provided later in this chapter.

Canada's National Cybersecurity Strategy and the Canadian Centre for Cyber Security

Introduced in 2018, Canada's new National Cybersecurity Strategy is the current government roadmap for protecting Canadian citizens, businesses and critical infrastructure from cyber threats. This strategy triggered substantial national investments in cybersecurity, totalling more than CAD 500m (approx US$366m) over five years, to sustain: the funding of the Canadian Centre for Cyber Security (CCCS, the federal government's technical authority, responsible for implementing certain key elements of the strategy), the creation of a National Cybercrime Coordination Unit and the funding allocated to innovation and economic growth in Canada. The CCCS provides expert advice, guidance, services and support on cybersecurity for government, critical infrastructure owners and operations, the private sector and the general public,[3] including to ensure the protection of computer networks and electronic information. The sharing of cybersecurity information with the government is encouraged in Canada; individuals, organisations and federal institutions can report incidents to the CCCS online. The CCCS collaborates with private sector organisations and shares threat information with private organisations through the Canadian Cyber Threat Exchange.[4] The CCCS also publishes

1 Government of Canada, Canada's Digital Charter, 2022 https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world accessed on 27 May 2024.
2 Parliament of Canada, Bill C-27, Summary https://www.parl.ca/legisinfo/en/bill/44-1/c-27 accessed on 27 May 2024.
3 Government of Canada, CCCS https://www.cyber.gc.ca/en accessed on 27 May 2024.
4 Canadian Cyber Threat Exchange https://cctx.ca accessed on 27 May 2024.

alerts and advisories on the latest threats,[5] as well as practical guidance about security measures[6] to be implemented by organisations and government agencies on topics such as tokenisation,[7] cryptography[8] and cloud-based security.[9]

There is no statutory requirement for private sector organisations to follow the CCCS guidance and this has not been specifically recommended by any of the relevant regulators. In practice, organisations in Canada often look to international standards, such as the standards developed by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) (as further detailed below).

Privacy legislation

The collection, use and disclosure of personal information[10] by private sector organisations in Canada is governed by the following statutes (collectively Canadian privacy laws): (1) PIPEDA; (2) Alberta's Personal Information Protection Act (Alberta PIPA); (3) British Columbia's Personal Information Protection Act (BC PIPA); and (4) Québec's Act on respecting the protection of personal information in the private sector (Québec Privacy Act). Depending on the circumstances, more than one Canadian privacy law might apply to an organisation's personal information practices. However, as recalled by the OPC, '[a]ll businesses that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province or territory in which they are based'.[11] Given the unlimited nature of metaverse worlds, the multiplicity of stakeholders involved and the different technologies used (hardware, software, distributed ledger technology (DLT)/blockchain, etc), there are great chances that the first largely accessible platforms (and organisations using such platforms to provide products and services) will handle personal information that will eventually cross provincial or national borders (to be processed by multiple third-party service providers for example). This explains the growing collaboration between the OPC and its regulatory counterparts[12] through partnerships.[13] In this regard, Canadian privacy laws: (1) require the implementation and maintenance of security safeguards; and (2) include an obligation to notify the concerned individuals, privacy regulators and other relevant organisations where a breach of such safeguards causes serious harm to individuals. Since Canadian privacy laws are technology neutral, they would consequently apply to activities within the metaverse, which involve the potential collection and handling of large amounts of sensitive data, including personal information.

Security requirements

Canadian privacy laws reflect fundamental principles regarding the management of personal information that are relevant to cybersecurity in the metaverse, namely accountability and certain specific safeguards. The accountability principle provides that an organisation is accountable for personal information in its custody or under its control, including information that has been transferred to a third party for processing. The safeguards principle provides that an organisation must use security safeguards (including physical, organisational and technological measures), appropriate to the sensitivity of the personal information in the organisation's custody or control, to protect the information (regardless of the form in which the information is held) against loss, theft and unauthorised access, disclosure, copying, use or modification.

These requirements have been interpreted by the OPC in various decisions that would likely apply to the metaverse.[14] For instance in *Marriott*, the OPC insisted that security measures must include a process to handle network changes; access controls; logging and monitoring measures; information storage, including encryption and data minimisation; vulnerability

5 Government of Canada, CCCS, Alerts and advisories https://www.cyber.gc.ca/en/alerts-advisories accessed on 27 May 2024.
6 Government of Canada, CCCS, Cyber security guidance https://www.cyber.gc.ca/en/guidance accessed on 27 May 2024.
7 Government of Canada, CCCS, Guidance on using tokenization for cloud-based services (ITSP.50.108), October 2021 https://www.cyber.gc.ca/en/guidance/guidance-using-tokenization-cloud-based-services-itsp50108 accessed on 27 May 2024.
8 Government of Canada, CCCS, Cryptographic algorithms for Unclassified, Protected A, and Protected B Information – ITSP.40.111, March 2024 https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111 accessed on 27 May 2024.
9 Government of Canada, CCCS, Guidance on defence in depth for cloud-based services – ITSP.50.104, May 2020 https://www.cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services accessed on 27 May 2024.
10 Broadly defined under Canadian privacy laws as 'any information about an identifiable individual'.
11 OPC, PIPEDA in brief, May 2019 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief accessed on 27 May 2024.
12 Government of Canada, 'Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act', November 2020 https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/raa-rar.html accessed on 27 May 2024.
13 OPC, Provincial and Territorial Partnerships, November 2022 https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp-incoming/pd_20220627/7d_provincial-territorial accessed on 27 May 2024.
14 OPC, Interpretation Bulletin: Safeguards, June 2015 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-interpretation-bulletins/interpretations_08_sg accessed on 27 May 2024.

testing and assessment; organisational and governance measures; as well as anti-virus software and endpoint threat detection tools.[15] In the same vein, in *Loblaws*, the OPC insisted on ensuring that organisations implement measures to protect their systems, networks and data files, that they encrypt personal information in transit and at rest; maintain technical safeguards namely through patches; and implement a pre-approval process for any sub-processors.[16]

The 2019 *Facebook* decision[17] appears specifically relevant to the operation of metaverse platforms. In its findings, the OPC required that the social media organisation appointed teams tasked with overseeing Facebook platform operations, monitoring compliance with the platform's policy and taking enforcement actions where appropriate.

Breach notification requirements

Under PIPEDA, a breach of security safeguards is defined as the loss of, unauthorised access to or unauthorised disclosure of personal information resulting from a breach of an organisation's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards.

Organisations must report a breach to the OPC and notify the affected individuals when it creates a 'real risk of significant harm' (RROSH) to the individuals affected.[18] 'Significant harm' is defined under PIPEDA as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[19] The factors relevant to determining whether a breach of security safeguards creates a RROSH include: (1) the sensitivity of the personal information involved in the breach; and (2) the probability that the personal information has been, is being, or will be misused.[20]

In its breach reporting guidance, the OPC indicates questions to consider in determining whether there is a RROSH, such as what potential harms could accrue to the individual, who accessed or could have accessed the information, how long the information has been exposed, whether there is evidence of malicious intent (eg, theft, hacking) and whether the information was adequately encrypted.

In Alberta, British Columbia and Québec, provincial privacy legislation operates in lieu of PIPEDA. To date, only Alberta and Québec require notification of data breaches. Under the Alberta PIPA, an organisation with personal information under its control must, without unreasonable delay, notify the Office of the Information and Privacy Commissioner of Alberta (OIPC) of any incident involving the loss of or unauthorised access to or disclosure of the personal information, where a reasonable person would consider that there exists a RROSH to an individual as a result of the loss or unauthorised access or disclosure.[21] The OIPC may then require the organisation to notify the individuals affected, although organisations generally notify the OIPC and the individuals concerned at the same time.[22]

Under the Québec Privacy Act, organisations have an obligation to notify the individuals affected and the Commission d'accès à l'information (CAI) of any confidentiality incident that presents a risk of serious injury.[23] A confidentiality incident is defined as access to, use of or communication not authorised by the law of personal information, or the loss of personal information, or any other breach in the protection of such information.[24]

Organisations must keep records of all incidents affecting personal information, whether or not they create a RROSH. This applies for at least two years following their occurrence under PIPEDA, five years under the Québec Privacy Act, yet the Alberta PIPA is silent on this point. As mentioned earlier, since Canadian privacy laws are technology neutral, such requirements would be applicable to the metaverse.

Sectorial legislation

In some specific sectors, additional cybersecurity guidance and compliance rules are provided to organisations due to the additional risks their activities involve.

15 PIPEDA Report of Findings No. 2022-005.
16 PIPEDA Report of Findings No. 2019-003.
17 PIPEDA Report of Findings No 2019-002.
18 PIPEDA, s 10.1.
19 PIPEDA, s 10.1(7).
20 PIPEDA, s 10.1(8).
21 AB PIPA, s 34.1.
22 AB PIPA, s 37.1. 9.
23 Québec Privacy Act, s 3.5.
24 Québec Privacy Act, s 3.6.

As such, since 2013, Canadian Securities Administrators (CSA) have emphasised that Canadian reporting issuers (companies whose shares are publicly traded) are required to disclose material cybersecurity risks and cybersecurity incidents promptly and accurately as part of their continuous disclosure of material information under Canadian securities laws. In a multilateral staff notice issued in 2017,[25] the CSA highlighted the material risk to 61 per cent of publicly traded companies (constituents of the S&P/Toronto Stock Exchange (TSX)) represented by potential cybersecurity breaches. The notice also provided 'guidance on risk factor disclosure and incident reporting'.

Canadian financial institutions are also subject to additional reporting obligations. Since March 2019, the Office of the Superintendent of Financial Institutions (OSFI), an independent Canadian federal government agency that regulates and supervises federally regulated financial institutions, has required these institutions to promptly report a technology or cybersecurity incident that is assessed to be of a 'high or critical severity level' (within 72 hours). Similar requirements were proposed by the Investment Industry Regulatory Organization of Canada (IIROC), the national self-regulatory organisation which oversees investment dealers and their trading activity in Canadian markets, with regards to its dealer members.

Finally, a federal bill known as Bill C-26, currently at the report stage in the House of Commons,[26] proposes the enactment of a Critical Cyber Systems Protection Act (CCSPA), which would provide 'a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety'. Part of the proposed changes include the requirement to establish a cybersecurity programme in respect of the critical cyber system[27] and mandatory cybersecurity incident reports[28] to the Communication Security Establishment (CSE)[29] within a maximum of 72 hours (or more, depending on future regulatory provisions).

These sectorial cybersecurity rules may be of interest to metaverse stakeholders, as some of the biggest platform developers may be publicly traded companies. Furthermore, one could easily imagine that financial institutions, investment dealers or even critical infrastructure service providers may be interested, in future, to render or obtain services through metaverse platforms and, as such, should be knowledgeable of the additional risks involved in these activities.

International standards

In addition to complying with the applicable legislation and regulatory guidance, Canadian organisations handling personal information and, more broadly, large amounts of data, may find it useful to comply with more detailed technical and management-oriented guidelines, such as those provided by the ISO/IEC 27001 standard and the NIST Cybersecurity Framework (CSF).

ISO/IEC 27001 provides a set of detailed requirements that an information security management system should meet to show that it 'preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed an optional certification process'.[30]

NIST CSF 2.0, updated in February 2024, 'aims to help all organizations – not just those in critical infrastructure, its original target audience – to manage and reduce risks' related to cybersecurity through 'a suite of resources that can be customized and used individually or in combination over time as an organization's cybersecurity needs change and its capabilities evolve'. [31]

Because they will be dealing with large amounts of data, including highly sensitive personal data, organisations involved in the metaverse should consider complying with either or both international standards for security reasons, as well as to reinforce the confidence of the public in regard to their actions.

25 CSA Multilateral Staff Notice 51-347, Disclosure of cybersecurity risks and incidents, January 2017.
26 Parliament of Canada, Bill C-26 summary https://www.parl.ca/legisinfo/en/bill/44-1/c-26 accessed on 27 May 2024.
27 CCSPA, s 9.
28 CCSPA, s 17.
29 Government of Canada, Communications Security Establishment Canada ('Canada's national cryptologic agency, providing the Government of Canada with information technology security and foreign signals intelligence') https://www.cse-cst.gc.ca/en accessed on 27 May 2024.
30 ISO, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, https://www.iso.org/standard/27001 accessed on 27 May 2024.
31 NIST, 'NIST Releases Version 2.0 of Landmark Cybersecurity Framework', 26 February 2024 https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework accessed on 27 May 2024.

2. What are the security-by-design principles applicable to the metaverse in your jurisdiction?

While security-by-design and privacy-by-design are well-established concepts in regulators' recommendations and guidance, they are not specifically required as such in Canadian privacy laws. The Québec Privacy Act refers to this concept only in a very limited way, by requiring that the privacy settings of an organisation collecting personal information when offering a technological product or service to the public be set-up 'by default', so as to provide 'the highest level of confidentiality'.[32] As such, while this provision requires the implementation 'by default' of the most protective security settings, it does not demand this level of protection from the early stages of development of the technological product or service and, as such, does not fully incorporate all seven privacy-by-design principles, which are: (1) proactive not reactive, preventative not reactive; (2) privacy as the default setting; (3) privacy embedded into the design; (4) full functionality; (5) end-to-end security; (6) visibility and transparency; and (7) respect for user privacy.

Recommendations from the OPC 2018-2019 Annual Report considers that privacy-by-design is an essential component of the accountability principle enshrined in Schedule 1 of PIPEDA: '[a]ccountability involves building privacy assurance into the very design of a product, service or initiative, from the early phase of conception through to its execution, deployment and beyond'.[33]

Furthermore, in its February 2018 report (Law 25 or the Privacy Legislation Modernization Act), the parliamentary Standing Committee on Access to Information, Privacy and Ethics (ETHI),[34] titled *(Law 25 or the Privacy Legislation Modernization Act)*, in recommendation 14, considers that all of the seven principles of the privacy-by-design concept should be included in PIPEDA. Despite such a recommendation, the Digital Charter Implementation Act does not include any reference to privacy-by-design principles.

More recently, on 13 April 2023, the CSE partnered with the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and other international partners to provide, in a guide, secure-by-design and secure-by-default principles to help technology manufacturers and suppliers in the development of their products.[35] The guide distinguishes between security-by-design and security-by-default and suggests that both concepts should apply to technology products to ensure they are 'safe for everyone'. Secure-by-design means, according to this guide, that 'security is built in from the development, not as an afterthought' and secure-by-default signifies 'products that are safe to use out of the box with little to no configuration changes necessary and are available without additional cost'.

Some cybersecurity guidance was further provided within the Voluntary Code of Conduct of the Responsible Development and Management of Advanced Generative AI Systems,[36] acting as an interim set of principles before the AI Act becomes binding legislation. Whereas this code does not specifically refer to the security-by-design or privacy-by-design principles, the listed recommendations suggest that cybersecurity and privacy measures should be considered during the entire engineering process of generative AI systems (and high-impact AI systems). This guide suggests that several measures should be implemented, such as the setting up 'of proportionate measures to mitigate risks of harm, such as by creating safeguards against malicious use'.

Finally, international standards (including the NIST Privacy Framework and ISO 31700) provide guidelines to help organisations integrate privacy-by-design principles.

As such, mandatory provisions to abide by the privacy-by-design principle in Canadian privacy laws are very limited (except for the privacy as the default setting principle embedded in Section 9.1 of the Québec Privacy Act) and metaverse stakeholders may refer to regulatory guidance and international standards and recommendations to ensure their products and services integrate security-by-design and privacy-by-design principles.

32 Québec Privacy Act, s 9.1.

33 OPC, 2018-2019 Annual Report https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf accessed on 27 May 2024 accessed 27 May 2024.

34 House of Commons Canada, ETHI Committee Report 'Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act', February 2018 https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12 accessed on 27 May 2024.

35 Cybersecurity and Infrastructure Security Agency, 'Shifting the balance of cybersecurity risk: principles and approaches for secure by design software' https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf accessed on 27 May 2024.

36 Government of Canada, 'Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems', September 2023 https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems accessed on 27 May 2024.

Q 3. Have there been any cyber incidents in the metaverse in your jurisdiction? How do the applicable policies, strategies or regulations react to cyber incidents?

As previously discussed, metaverse technology poses multiple questions in terms of cybersecurity and creates increased risks of cyber incidents due to the multiple stakeholders involved, the volume and sensitivity of the personal information collected, held and transferred through metaverse platforms, and the high-risk technologies involved. This includes, for instance, technologies tracking and analysing the behaviour and emotions of individuals connecting to the metaverse to access products or services.

Because metaverse platforms are not yet used by a large proportion of the public (except for in the video games sector), as of the date this chapter was drafted, no cyber-incidents in the metaverse have been publicly reported in Canada.

Whereas Canadian privacy laws do not directly provide sanctions for cyber incidents, they sanction contraventions by organisations of the security safeguard provisions they enshrine, with such contraventions possibly resulting in cyber incidents.

As such, Section 28 of PIPEDA, states that an organisation that knowingly infringes obligations concerning the retention of information,[37] that does not comply with the obligation to report a breach of security to the OPC when required,[38] that does not keep a record of such breaches as required by law,[39] that retaliates against an employee because of the denunciation of an irregularity to the OPC or because such employee refuses to violate the provisions of the law,[40] or that obstructs the OPC 'in the investigation of a complaint or in conducting an audit', may be found guilty of a maximum offence of CAD 100,000. Monetary penalties under PIPEDA are not administrative sanctions, they result from judicial proceedings initiated before the Federal Court. Usually, a complaint is investigated by the OPC, which then, if appropriate, prepares a report and such report is sent to the complainant and to the organisation. An application to the Federal Court can then be filed by the OPC (or by the complainant).[41] In addition to the abovementioned monetary penalties, the Federal Court can also 'order an organization to correct its practices', 'order an organization to publish a notice of any action taken or proposed to be taken to correct its practices' and 'award damages to the complainant, including damages for any humiliation that the complainant has suffered'.[42]

While the Alberta PIPA and BC PIPA provide for the same offence amount and a similar sanctioning process as PIPEDA, the Québec Privacy Act largely increased the amounts applicable to organisations found in violation of its provisions by imposing administrative sanctions of up to CAD 10m, or two per cent of the worldwide turnover of the company for the preceding fiscal year, if greater.[43] Consequently, the CAI may require administrative penalties to be issued to organisations when, among other infringements listed in Section 90.1, a confidentiality incident is not reported to the CAI or to the concerned individuals or when an organisation 'does not take the security measures necessary to ensure the protection of the personal information' that are 'collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored'.[44]

In addition to these administrative penalties, the Québec Privacy Act includes penal offences for the most serious violations (including the abovementioned default in terms of incident reporting and a lack of security measures) which can be as high as CAD 25m, or four per cent of worldwide turnover of the company for the preceding fiscal year, if greater.[45] Punitive damages of no less than CAD 1,000 may also apply when a violation of the Québec Privacy Act 'causes an injury and the infringement is intentional or results from a gross fault'.[46] These monetary sanction provisions result from an amendment to the Québec Privacy Act which came into force on 22 September 2023. As such, no CAI decision imposing such penalties existed at the time this chapter was drafted.

37 PIPEDA, s 8(8).
38 PIPEDA, s 10.1.
39 PIPEDA, s 10.3(1).
40 PIPEDA, s 27.1(1).
41 PIPEDA, ss 14 and 15.
42 PIPEDA, s 16.
43 Québec Privacy Act, s 90.12.
44 Québec Privacy Act, s 10.
45 Québec Privacy Act, s 91.
46 Québec Privacy Act, s 93.1.

In a 2021 class action decision by the Superior Court of Ontario,[47] opposing Yahoo Inc and the alleged victims of multiple cyberattacks against its worldwide databases, the judge recalled the necessity of actual harm resulting from a cyberattack to award damages to class action members (five million Canadians): 'It should be observed that it is always the case that the extent of potentiality and the actuality of harm from cyberattacks is unknown, unknowable, or capable of being proven only with considerable difficulty'. A settlement of around CAD 20.3m was approved for the five million class members, with a per capita value of CAD 4 per class member. In other words, it was almost a symbolic amount given the volume of data hacked.

Q 4. Are there any cybersecurity standards in your jurisdiction specifically applicable to the metaverse? What are the main obligations they set out?

As of the date this chapter was drafted, no cybersecurity standards specifically applicable to the metaverse exist in Canada.

Q 5. Are there any upcoming policies, strategies or regulations that will impact cybersecurity in the metaverse?

The main upcoming policies, strategies or regulations in Canada that may affect cybersecurity in the metaverse include the enactment of the CCSPA (mentioned above) under Bill C-26 and the CPPA, the AI Act and the Tribunal Act, under Bill C-27 or the Digital Charter Implementation Act (mentioned above).

The CCSPA, as further detailed above, according to its stated purpose, aims to protect 'critical cyber systems in order to support the continuity and security of vital services and vital systems by ensuring that' cybersecurity risks are identified, and incidents are managed and minimised.[48] Vital systems and services include telecoms services, pipeline and power line systems, nuclear energy systems, transport systems and banking systems.[49]

The CPPA includes a series of substantial changes to the current private sector privacy provisions contained in PIPEDA, aimed at modernising 'Canada's legislative framework so that it is suited to the digital age'.[50] While implementing PIPEDA's Schedule 1 principles, including the security safeguards principle and the breach notification requirement, the CPPA places several additional privacy obligations on organisations, such as 'the development of a privacy management program and data minimization obligations'.[51] The CPPA also introduces new provisions that are relevant to cybersecurity, namely new exceptions to the default consent requirement for activities that are 'necessary for the organization's information, system or network security' or 'necessary for the safety of a product or service that the organization provides';[52] a right to erasure,[53] obligations as to the de-identification of personal information;[54] significant administrative monetary penalties of up to CAD 10m (or three per cent of the company's worldwide gross revenue if higher); as well as new powers for the OPC (including the ability to issue orders and to recommend the amount of the administrative penalty to be imposed on infringing organisations);[55] and criminal fines of up to CAD 25m in the case of contraventions by organisations of certain provisions of the CPPA (including, for example, the failure to report breaches to the OPC and affected individuals and the failure to maintain breach records).[56] The CPPA also introduces a private right of action giving 'a cause of action for damages to an individual affected by the acts or omissions of an organization that has contravened the CPPA'.[57]

47 *Karasik et al v Yahoo! Inc* 2021 ONSC 1063.
48 CCSPA, s 5.
49 CCSPA, sch 1.
50 Parliament of Canada, Bill C-27 summary, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E#a2-1 accessed on 27 May 2024.
51 *Ibid*.
52 CPPA, s 18(2).
53 CPPA, s 55.
54 CPPA, ss 74 and 75.
55 CPPA, s 93 to s 95.
56 CPPA, s 128.
57 Parliament of Canada, Bill C-27 summary https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E#a2-1 accessed on 27 May 2024.

The Tribunal Act proposes to establish a new tribunal competent to rule on appeals to the OPC's decisions, findings or orders, and for imposing administrative penalties as per provided in Section 95 of the CPPA.

The AI Act aims to regulate 'international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems' and prohibit 'certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests'.[58] As such, the AI Act requires that any artificial intelligence system shall be assessed by the organisations responsible for such system to determine whether it is a high-impact systems (this term will be defined in further regulation).[59] If such system is a high-impact system, then obligations concerning mitigation measures[60] and to keep records of such measures will apply.[61] Violations of the AI Act will be sanctioned by administrative penalties of amounts to be determined by further regulations.[62]

Finally, the Ontario government issued, in 2020, a discussion paper on a new private sector privacy law, followed by a white paper titled 'Modernizing Privacy in Ontario – Empowering Ontarians and Enabling the Digital Economy', which suggests a real interest in introducing a bill in the Ontarian legislative assembly. Should such an act be enacted, it would, subject to being deemed substantially similar to the federal legislation (now PIPEDA and then the CPPA), apply to businesses conducting commercial activity within Ontario and would be the fourth provincial private sector privacy law in Canada.

As recalled throughout this whole chapter, Canadian legislation is technologically neutral and, as such, the abovementioned provisions will apply to the metaverse once enacted. Given the potential use of many AI-based technologies in the context of the metaverse, including to enable interactions and secure identities within authentication processes, the coming into force of the AI Act (and the future regulations related to the AI Act) should be monitored by all metaverse stakeholders.

Last updated: 30 April 2024.

58 AI Act, s 4.
59 AI Act, s 8.
60 AI Act, s 9.
61 AI Act, s 10.
62 AI Act, s 29(1).

Intellectual property

James Buchan *Gowling, Toronto, Ontario*

1. What are the public policies, strategies or regulations relating to intellectual property which are applicable to the metaverse in your jurisdiction?

Intellectual property (IP) laws, policies and regulations, such as copyright, trademark and patent laws, generally apply to digital content and creations within the metaverse. However, there are no specific regulations currently directed specifically to the metaverse in Canada.

Within the Canadian context, the following are the key considerations relating to IP in the metaverse:

- copyright – existing copyright laws protect original works of authorship, including literary, artistic and musical works. Copyright may apply to virtual objects, avatars, music and other digital content. Copyright law in Canada also addresses issues related to reproduction, distribution and public performance of digital content;
- trademarks – trademark laws protect distinctive marks (eg, typically words and/or designs) used to identify goods or services. In the metaverse, trademarks may apply to virtual marks, such as brands, logos and symbols, associated with virtual goods or services;
- patents – Canadian patent laws protect new, useful and unobvious inventions. While traditional patents may not directly apply to virtual environments, innovations related to technology that supports the metaverse may be subject to patent protection; and
- trade secrets – the protection of trade secrets is relevant to safeguard confidential information. In the metaverse, creators may have proprietary algorithms, virtual designs or other confidential information that requires protection.

2. How are intellectual property rights to 'virtual objects', 'buildings' and 'avatars', etc, protected in your jurisdiction?

IP rights to virtual objects, buildings, avatars and other elements within the metaverse may be protected through existing IP laws in Canada. Considerations for different types of virtual entities include the following:

Virtual objects

Virtual objects, which can include digital art, 3D models and other creative works, may be protected by copyright. The creator of the virtual object holds the copyright, and reproduction, distribution and public display rights are protected. The owners of virtual objects may use licensing agreements to grant others the right to use, modify or distribute their creations within the metaverse.

Virtual buildings

The architectural design of virtual buildings may be protected by copyright. The creator of the virtual building may have rights over its reproduction and public display. If virtual buildings represent brands or businesses, trademark protection may apply to distinctive visual elements associated with the buildings. Similar to virtual objects, licensing agreements can be used to control the use of virtual buildings within the metaverse.

Avatars

The visual appearance and design of avatars may be protected by copyright. Avatars created by users may be subject to their copyright, while platform creators may hold rights over default avatars. If avatars represent a brand or identity within the metaverse, trademark protection may be applicable. In some cases, the likeness or persona of an individual represented by an avatar may be protected under personality rights. Virtual worlds often have terms of service that outline the rights and limitations regarding avatars present within the platform.

Q 3. How are digital replicas of physical objects protected in your jurisdiction?

Digital replicas of physical objects (eg, digital twins) may be protected in Canada through various traditional IP mechanisms and related legal considerations. The protection afforded to such digital replicas typically involves copyright, but may involve other adjacent IP rights.

To be eligible for copyright protection in Canada, a digital replica must meet the originality requirement, meaning it is the result of independent creative effort and possesses a degree of skill and judgement. This can include artistic or creative elements of the digital representation. The creator or the entity commissioning the creation of the digital replica typically owns the copyright. Copyright provides exclusive rights to reproduce, distribute and display the digital replica. Unauthorised copying or use may constitute copyright infringement.

Owners of digital replicas may use licensing agreements to control the use and reproduction of the digital twin by others. Licensing agreements can specify the terms and conditions under which the digital replica can be used.

Q 4. How is user-generated content and other derivative works protected in your jurisdiction?

User-generated content (UGC) and derivative works are generally protected under copyright law in Canada. The Canadian Copyright Act governs the rights of creators and users of copyrighted works.

For copyright protection to apply, the user-generated content or derivative work must meet the originality requirement, namely the work must be the result of independent creative effort and not a copy of existing works. The individual who creates the work (eg, UGC) is typically considered the author and owner of the copyright in Canada, provided the work meets the originality criterion and the work was not created by an employee in the course of their employment or otherwise governed by a contract.

Derivative works, namely new works created by modifying or adapting existing works, may also be protected by copyright law in Canada. This includes works based on pre-existing material, such as translations, adaptations or remixes.

The copyright owner of UGC or derivative works has exclusive rights to reproduce, distribute, perform and display the work. Others need the copyright owner's permission to use these rights. In addition to economic rights, Canada recognises moral rights, including the right of attribution and the right to the integrity of the work. Moral rights protect the personal and reputational interests of the creator.

The Canadian Copyright Act includes provisions for fair dealing, which allows users to engage in certain activities for specific purposes without infringing copyright. Fair dealing exceptions may include research, private study, criticism, review and news reporting.

In addition to copyright law, creators of UGC must also be mindful of licensing considerations, including the terms of service of platform operators. Platforms hosting UGC often have terms of service that outline the rights and obligations of users.

Q 5. Are there any collective rights management organisations active in your jurisdiction that also manage intellectual property rights on the metaverse?

Collective rights management organisations in Canada handle IP rights that may claim jurisdiction to the metaverse. These organisations typically administer and enforce the rights of creators by managing licences, collecting royalties and ensuring compliance with copyright laws. However, the specific involvement of such organisations in managing IP rights in the metaverse is an emerging area.

The prominent collective rights management organisations in Canada that traditionally handle IP rights include:

- the Society of Composers, Authors and Music Publishers of Canada (SOCAN) – SOCAN manages the rights of music creators and publishers, including the collection and distribution of royalties for the public performance of musical works;
- Access Copyright – Access Copyright is involved in the collective administration of copyright for literary works, including text-based content, such as books, articles and other written materials; and
- The Canadian Musical Reproduction Rights Agency (CMRRA) – which manages the reproduction rights of musical works on behalf of music publishers and copyright owners.

Q 6. How are intellectual property rights protected and enforced on the metaverse in your jurisdiction?

The protection and enforcement of IP rights in the metaverse in Canada is presumptively governed by existing statutory IP laws. However, the application of existing IP laws to virtual environments presents unique and untested challenges and considerations. As noted above, the statutory protection of IP rights is typically conferred by copyright, trademark and patent laws. The enforcement of those rights is typically pursued through civil litigation against infringers for remedies such as injunctions, damages or an account of profits.

Q 7. Are there any intellectual property strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote interoperability in the metaverse?

Currently there are no specific IP strategies, policies or regulations in Canada explicitly aimed at promoting interoperability in the metaverse.

Q 8. Are there any competition strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote standardisation and access to fair and non-discriminatory licenses?

Currently, there are no specific competition strategies, policies or regulations in Canada aimed at promoting standardisation and access to fair and non-discriminatory licences within the metaverse in Canada. However, broader competition law principles and regulations may indirectly address issues related to standards and fair licensing practices.

Canada's competition law, primarily governed by the Competition Act, aims to maintain and encourage fair competition. The general provisions of the Canadian Competition Act apply to anti-competitive behaviour, including practices that may hinder standardisation or fair licensing. For example, the Competition Act includes provisions related to a refusal to deal, abuse of dominance, exclusive dealing, tied selling and market restrictions. If a user in the metaverse is deemed to be in a position of dominance and engages in conduct that lessens or prevents competition, this could be subject to scrutiny by the Canadian Competition Bureau. Agreements among entities in the metaverse that harm competition,

hinder standardisation or lead to discriminatory licensing practices may also be subject to review and investigation by the Canadian Competition Bureau. Non-compliance with competition law may result in civil and administrative sanctions. This can include fines, injunctions and other remedies to address anti-competitive practices.

Q 9. Are there any other intellectual property issues related to the metaverse that have been addressed in your jurisdiction?

While the traditional statutory regimes which protect IP rights in Canada provide the legal backdrop to governing and regulating IP issues generally, there are a number of other circumstances unique to the metaverse that will raise IP-related issues. For example, issues relating to IP ownership, transfer and licensing arise in the context of digital artwork related to non-fungible tokens (NFTs). Establishing the legal status of digital goods and services has yet to be addressed in Canada.

Q 10. What are the roles of metaverse providers?

The roles of metaverse providers are multifaceted. Metaverse providers must create a compelling and user-friendly virtual environment, while addressing legal, ethical and technical challenges. The ecosystem involving metaverse providers will include technology companies, platform operators and service providers who are all involved in developing, hosting and maintaining the infrastructure that enables virtual interactions. The roles of these providers vary and overlap, but create an ecosystem of operators involved in the design, support, maintenance and compliance of the metaverse. For example, platform developers design and develop the underlying technology infrastructure and software platforms that enable users to access and engage with the metaverse. Designers create virtual worlds or environments to allow users to interact, socialise and engage in various activities in the virtual world. Together, these metaverse providers create user experiences in the virtual world which allow users to navigate, communicate and interact with each other and with other assets and features in the virtual world. Metaverse providers must also comply with all relevant legal and regulatory frameworks, including intellectual property laws, privacy regulations and all other jurisdiction-specific requirements.

Q 11. How does your jurisdiction moderate content and how does it balance this with freedom of expression?

The balance between content moderation and freedom of speech in the metaverse is a complex and nuanced issue. Content moderation, namely the practice of monitoring, reviewing and managing UGC on digital platforms, can include removing or restricting UGC or commentary that violates community guidelines, terms of service or legal standards. The interests of content moderation are occasionally in tension with users' rights to freedom of speech and expression.

In Canada, freedom of speech is a protected fundamental right under the Canadian Charter of Rights and Freedoms, part of the Canadian Constitution. Section 2(b) of the Charter specifically guarantees freedom of expression, including freedom of speech, freedom of the press and freedom of peaceful assembly. This protection encompasses a wide range of forms of expression, including verbal, written, artistic and symbolic communication.

Many platforms in the metaverse use automated content moderation systems powered by algorithms. These systems can be maladroit to accurately distinguishing context, satire or nuanced expressions, potentially leading to censure, impacting fundamental rights of speech or expression by users. The Canadian government is likely to introduce and pass legislation imposing content moderation requirements on platform operators to reduce harm, while attempting to balance the constitutionally protected freedoms of users in Canada.

Q 12. Are there any by-design notice mechanisms?

'By-design notice mechanisms', namely the act of incorporating incorporating notice and transparency elements directly into the design of products, services or systems, aim to provide users with clear information about data practices.

While general privacy principles are applied in Canada, the specific term 'by-design notice mechanisms' is not explicitly outlined in PIPEDA, the key privacy law statute in Canada, which addresses the collection, use and disclosure of personal information by private sector organisations (see the chapter on data).

13. Are there any upcoming policies, strategies or regulations relating to intellectual property in your jurisdiction?

There are currently no upcoming policies, strategies or regulations impacting IP per se in Canada relating to the metaverse. However, in June 2022, the Government of Canada tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act 2022. AIDA represents an important milestone in implementing the Digital Charter and ensuring that Canadians can trust digital technologies. The design, development and use of AI systems must be safe and must respect the values of Canadians.

The framework proposed in AIDA is the first step towards a new regulatory system designed to guide AI innovation in a positive direction, and to encourage the responsible adoption of AI technologies by Canadians and Canadian businesses. The government intends to build on this framework through an open and transparent regulatory development process. Consultations to gather input from a variety of stakeholders across Canada, to ensure that the regulations achieve outcomes aligned with Canadian values, are currently underway.