

mccarthy tetrault

Technology Perspectives Outlook

2026

mccarthy tetrault

This publication reviews key developments in Canada during 2025, and their potential impact in 2026 and beyond. For further information, please speak to one of our authors.

Co-Editors:
Robert Anton and Michael Scherman

Authors:
Bronte Anderson, Elle Anderson, Robert Anton, Connor Bildfell, Jade Buchanan, Shashank Chaddha, David Crane, Matthew Cumming, John Durland, Daniel Glover, Christine Ing, Vanessa Johnson, Gillian Kerr, Francis Langlois, James Lin, Mehak Merchant, Mohammed M'Hiri, Charles Morgan, Michael Scherman, Michael Shahinian, Lori Stein and Julie Watts.



TABLE OF CONTENTS

Tech Outlook 2026: Introduction	01
Venture Market Update	02
Corporate Venture Capital and Strategic Investments in High-Growth Tech Companies	04
Digital Infrastructure Investment in Canada	07
Open Banking in Canada: The Journey, the Present, and the Emerging Road Ahead	08
Canada's Stablecoin Act: A Bold Step Forward	10
Navigating Canada's Evolving Payments Regulatory Landscape	14
Hot Topics in Privacy and Cybersecurity	17
Trends in AI Litigation: Lessons for 2026	20
Getting "IT" Right the First Time: How Early Decisions Determine the Success of Technology Projects	22

Tech Outlook 2026: Introduction

AI, digital infrastructure and tech buildouts continue to dominate not only the tech sector but the economy as a whole. We cover how this is affecting the Canadian tech sector, both on a macro and individual business level, as well as the lingering litigation risks. This has been and remains a focus at the executive level as businesses look to optimize their products and streamline their operations.

On the corporate transaction side of things, our Venture Market Update provides our annual update and assessment of the venture capital markets in Canada. In short, the race for AI winners has led to fewer, but larger, transactions and investments. And as perceived winners have increasing access to private capital, strategics are growing their presence in private-company financings. The implications of this are discussed in our second piece, Corporate Venture Capital and Strategic Investments in High-Growth Tech Companies.

On a macro level, the digital infrastructure buildout that has dominated headlines with high dollar investments and aggressive projections follows in our next piece, Digital Infrastructure Investment in Canada (shared with our Private Equity Outlook), which describes how that buildout is tracking in Canada. Meanwhile, in the marketplace, the litigation risks of generative AI continue to play out in Canadian courts.

Next, we have three great pieces on three rapidly-evolving areas: open banking, crypto and payments:

— Open Banking in Canada: The Journey, the Present, and the Emerging Road Ahead describes the past, present and future of this potentially major transformation to Canada's financial and payments landscape.

— Canada's Stablecoin Act: A Bold Step Forward gives an update on another potentially transformative regulatory change, this time to the Canadian cryptocurrency market, that could pave the way to Canadian dollar-denominated stablecoins.

— Navigating Canada's Evolving Payments Regulatory Landscape details the opportunities in Canada's changing payments-regulatory space, as well as new compliance challenges that will be present.

We also cover the omnipresent regulatory risks for Canadian tech businesses dealing with privacy and cybersecurity in Hot Topics in Privacy and Cybersecurity – a critical area to stay on top of as technologies and legal requirements are evolving faster than ever.

For our final pieces, Trends in AI Litigation provides an update and analysis on the roiling litigation issues affecting generative AI businesses, while Getting "IT" Right the First Time focuses on individual businesses looking to undertake large-scale IT projects and highlights trends and best practices in implementing them successfully.

Robert Anton, Co-Editor
Michael Scherman, Co-Editor





Venture Market Update

CONTINUED SHIFT TOWARD FEWER, LARGER AND MORE SELECTIVE INVESTMENTS

In 2025, the venture capital ("VC") market continued to see fewer, larger and more targeted investments, with capital increasingly concentrated among the companies demonstrating strong growth and operational resilience – especially those in the artificial intelligence ("AI") sector. Investors showed a clear preference for businesses with proven fundamentals, and the AI sector stood out as a magnet for capital. The valuation step-ups for AI were generally present across industries. For example, during the first half of the year, early-stage AI fintechs attracted higher valuations and larger rounds, seeing a median valuation of US$134 million compared to a median valuation of US$39.2 million of their non-AI peers – a 242% premium – in the U.S. VC market.

As a consequence of the investor preference of quality over quantity, overall venture activity in Canada generally declined. By the end of the third quarter, total investment reached C$4.9 billion across 386 deals, a drop from C$8.6 billion in 2024 and C$7.1 billion in 2023. The third quarter, however, did see a rise in investment amounts, with C$1.8 billion across 123 deals, but this increase was driven by a handful of mega-deals at the growth stage rather than a broad-based recovery. One notable financing involved Cohere, an AI company that secured US$600 million at a US$7 billion valuation. Many of these mega-deals were denominated in U.S. dollars, underscoring the ongoing influence of American investors in the Canadian VC market.

On the fund side, the pool of dry powder in Canada appears to be shrinking, Canadian VC fundraising is down, and the share for new investments (relative to follow-ons and secondaries) has dropped significantly. The increased prevalence of follow-ons and secondary funds and transactional activity reflects the market's current focus on quality investments later in the growth cycle. In 2022, 81% of dry powder was available for initial investments, but by 2025, that figure had fallen to 42%. This change is partly a result of the timing of capital raised during the fundraising boom of 2021 and 2022, which is now locked up for reserves. Since Canadian VC fundraising has declined, this leaves less fresh capital to support early-stage startups in 2026.

DEAL ACTIVITY AND EXITS

Debt financing played a prominent role throughout 2025, with C$717 million raised across 50 deals by the end of the third quarter. Venture debt and convertible debt remained strong sources of capital in the first half of 2025, especially among later-stage and growth-stage companies, with

activity slowing down in the third quarter as founders shifted back toward equity rounds. These forms of non-dilutive or less-dilutive capital allowed founders to extend their runway and navigate periods of uncertainty, including the tariff negotiations and ongoing trade tensions. By leveraging debt, many companies were able to bridge gaps between equity rounds and position themselves for future growth without immediately impacting ownership.

With the exception of growth-stage investment activity, venture investment activity across most stages showed a general decline, with early-stage investment activity lagging behind the broader market the most. Seed-stage investment activity, while demonstrating some resilience in terms of total dollars invested, experienced a drop in deal volume and a decline in overall investment compared to previous years. This slump reflects tighter market conditions and increased selectivity among institutional investors. Conversely, growth-stage investment activity has increased, with growth-stage deal volume up 71% year over year. Investors are prioritizing companies with established business models and clear paths to scale, resulting in larger rounds and more robust capital deployment at this stage.

The exit environment in Canada remained subdued, with no VC-backed initial public offerings ("IPOs") recorded in 2025. Liquidity was primarily generated through M&A deals and secondary sales, such as Clio's fundraising round to, in part, finance the acquisition of vLex at US$1 billion. As companies stayed private for longer periods, secondary transactions became a key mechanism for providing liquidity to founders, employees and early backers. These transactions account for a significant portion of the exit value in 2025, and demand for secondary transactions is expected to remain strong as investors seek alternative paths to liquidity. By the end of the third quarter, M&A deals represented roughly 80% of exits even though disclosed values were generally modest. Meanwhile, the U.S. market saw a wave of VC-backed companies going public, with 13 IPOs as of mid-August 2025 compared to eight in 2024 – a sign of renewed momentum. With the IPO market poised for further growth in 2026, there is optimism for Canadian start-ups.

DEAL TERMS

In previous years, as the VC market corrected post-Covid, investor-friendly provisions became commonplace as down rounds and valuation resets swept through the market. However, as conditions have continued to stabilize, deal terms and structures are gradually returning to the norms seen before the pandemic. Protective terms such as pay-to-play and participating liquidation preferences continue to be less prevalent. This shift reflects renewed confidence in the market and a more competitive environment for high-quality companies.

TRENDS HEADING INTO 2026

AI remains the standout sector, attracting the largest share of venture capital and commanding premium valuations. Investors are prioritizing companies that leverage AI for productivity, automation and new business models. Growth-stage AI firms continue to secure substantial rounds, and the sector's momentum is expected to persist as both Canadian and global investors prioritize innovation in this space.

Cleantech investment has declined to its lowest level since the pandemic, with capital focused on specific areas such as thermal and geothermal technologies. Despite these challenges, policy initiatives around energy and infrastructure may open new avenues for growth in the coming year.

A major shift is underway in defence and security, driven by new government priorities. The Defence Industrial Strategy, backed by a C$6.6 billion commitment, is designed to boost research, strengthen supply chains and make capital more accessible for companies working on advanced technologies in this sector. This initiative is expected to accelerate the development of solutions that serve both civilian and military needs, including AI, cybersecurity, quantum computing, and next-generation materials. As a result, the defence sector is poised for booming growth in 2026. Companies that can position themselves within national supply chains or offer advanced capabilities for defence operations are likely to dominate. The rising demand for electricity to power data centres and AI infrastructure further intersects with defence priorities, creating new opportunities for startups.

Heading into 2026, investors are expected to remain selective, with capital expected to flow toward sectors demonstrating resilience, capacity to scale and alignment with macro trends such as AI adoption. Government policy, infrastructure projects and global market dynamics will continue to shape sector priorities and investment opportunities

List of Sources: PitchBook, CVCA, Carta, EY, KPMG , PYMNTS, Yahoo Finance and S&P Global

Corporate Venture Capital and Strategic Investments in High-Growth Tech Companies

WHAT IS CORPORATE VENTURE CAPITAL?

Corporate venture capital ("CVC") refers to investments by established companies into growth-stage or emerging companies. In contrast to traditional venture capital funds that manage capital from their limited partners and seek to maximize the financial returns on the investment of such capital, CVC combines strategic intent with financial return and is guided by a single corporate parent's business strategy, which may involve investing in a company that provides strategic benefits to the corporate parent at large in addition to financial return. Strategic objectives that a corporate parent seeks to achieve through CVC may include, among other things, gaining access to new technologies, entering new markets, establishing an M&A pipeline, or fostering innovation relevant to the corporate parent's core business.

In Canada, corporate venture capital has evolved from a niche investment strategy into a mainstream corporate growth strategy. Increasingly, large enterprises have started deploying corporate venture capital as a vital strategy to gain access to emerging technologies, rather than relying solely on internal research and development.

THE CORPORATE VENTURE CAPITAL LANDSCAPE IN CANADA

Corporate venture capital is a growing and increasingly important part of Canada's innovation ecosystem. Although it is estimated that only about 6% of Canadian public companies with more than C$1 billion in annual revenue have an established corporate venture capital arm, deal participation by Canadian CVCs has nearly tripled in recent years, far outpacing growth in traditional venture capital activities.[1]

Although CVC investments have typically been concentrated in the financial services, technology and media and telecom sectors, such investment strategies have started to be adopted also by Canadian companies in the oil and gas, mining, and industrial sectors. This diversification reflects a broader trend: corporates now treat venture investment as a strategic lever for digital transformation and supply-chain capabilities. According to the Canadian Venture Capital & Private Equity Association, venture investment totaled C$2.9 billion across 254 deals in H1 2025, with average round sizes rising to C$11.4 million.[2]

Although CVC investing is a growing trend, growth-stage companies should view CVC as a supplement to the traditional venture capital model, rather than its replacement. As noted below, CVC investors usually participate as minority



1 Deloitte Ventures in collaboration with BDC, "***The state of corporate venture capital in Canada – Investing today to ignite tomorrow***" (May 2024), page 8.

2 Canadian Venture Capital and Private Equity Association, "***Canadian Venture Capital Market Overview H1 2025***", pages 5–6.

investors alongside institutional venture capital investors. Going forward, CVC is expected to continue to contribute to diversification within the venture capital ecosystem.

WHY CORPORATE VENTURE CAPITAL MATTERS NOW

Market volatility in recent years, the cost of borrowing decreasing, and companies facing valuation corrections[3] have encouraged private equity and venture capital investors to scrutinize deals more closely, conduct more rigorous due diligence, and generally deploy capital more selectively. This environment favours corporates that can diligence a company quickly and knowledgeably, invest directly from their balance sheets, and pursue long-term strategic objectives, rather than traditional funds that depend on quicker liquidity.

BENEFITS AND RISKS OF CORPORATE VENTURE CAPITAL INVESTMENTS

For corporates, CVC investing delivers both strategic and financial benefits. It creates a pipeline for partnerships and future acquisitions while offering early exposure to disruptive technologies. A minority stake in a promising startup lets the corporate investor test product-market fit and evaluate collaboration before committing to a control transaction. For startups, CVC funding delivers more than capital. It provides credibility, distribution support, and mentorship that can accelerate commercialization. A CVC backer's brand validation often makes customer acquisition and future fundraising easier.

However, CVC investments carry distinct risks. Large corporates must consider compliance and reputation risks alongside return on investment. A failed investment can reflect directly on the parent's credibility – as illustrated by Safeway and Walgreen's investment and partnership with Theranos, in which the fraudulent technologies of the blood-testing startup resulted in significant financial losses and reputational damages to the corporate investors. Because CVC stakes are typically minority positions, the corporate investor often lacks control over the startup.

For startup companies, or funds or other investors in startup companies, seeking capital from CVC investors, the main hazards of receiving CVC investments mirror those advantages. Bringing a potential competitor onto the cap table can deter other investors or acquirors and raise concerns about information leakage or intellectual property misappropriation. Startups and their investors must weigh the strategic value of corporate capital against the possibility of future conflicts or "soft landings" that benefit the strategic more than the startup.

Legal frameworks offer ways to balance these tensions. Under the Canadian venture capital model, the company's board of directors decides whether a shareholder qualifies as a competitor – a designation that can strip information and inspection rights, limit transfers, and curtail pre-emptive privileges. Clear competitor definitions and carve-outs for strategics can prevent unintended restrictions. Side letters remain the preferred tool for tailoring rights to specific corporate compliance obligations. Side letters may also include faster exit mechanisms – such as put rights triggered by regulatory or reputational events – to provide flexibility or protect brand integrity.

3 *Supra*, note 2, page 19.



VENTURE CAPITAL BASICS AND HOW CORPORATE VENTURE CAPITAL FITS

Venture-backed companies raise capital through a predictable sequence of securities issuances: founders contribute intellectual property and receive common shares, seed capital arrives via convertible notes or simple agreements for future equity (SAFEs), and subsequent priced rounds result in the issuance of convertible preferred shares with liquidation preferences and anti-dilution protections. Lead investors often receive board representation and "major investor" rights, including those with respect to financial reporting, budget access, and approval rights over key transactions. Major-investor status depends on ownership thresholds that vary by round and can fall away if investors are diluted below the negotiated percentage.

Within this framework, CVC investors usually participate as minority holders in priced equity rounds alongside institutional venture capital investors. CVC investors typically negotiate bespoke side letters to address information flows and their internal compliance needs without disrupting the broader shareholder governance framework.

CVC investments also take other forms. For example, a corporate may spin out technology into a new entity founded by former employees, and take a large early stake in exchange for the promising intellectual property. Netflix's creation of Roku is an example of how a corporate can monetize non-core innovation without hampering its main business. As well, sometimes CVC investments can take the form of convertible securities, such as warrants in the company issued in connection with the corporate's commercial partnership with the company.

EXITS FROM CORPORATE VENTURE CAPITAL INVESTMENTS

Exit pathways for CVC-backed companies generally mirror those of the broader venture market, but carry unique strategic dynamics. If the company undertakes a process, other bidders that may be competitors of the CVC investor may be dissuaded if they feel the CVC investor can block a transaction. This could potentially hinder return for other investors, including fund investors in the company. Alternatively, if the CVC investor is not interested in the acquisition, other bidders may be concerned that the company is flawed. Nevertheless, a common outcome is a strategic acquisition by the corporate investor itself, reflecting the CVC's dual interests in financial return and business integration. Processes where that is not going to happen need to be handled carefully and considerately.

Although initial public offerings are a desirable exit outcome for growth companies, corporates may prefer control or collaboration over the loss of influence that comes with an IPO, again potentially putting the CVC investor in conflict with fund investors. Finally, in more distressed situations, corporates may leverage their insight and proximity to acquire assets or teams from insolvency processes – a more unfortunate form of "soft landing" that preserves valuable intellectual property even when equity value has been lost.

LOOKING AHEAD TO 2026

CVC is expected to gain further traction in Canada as Canadian corporates formalize their programs and governance and to keep their M&A pipeline as more companies stay private longer. Future transactions are likely to feature sharper competitor definitions and explicit board-discretion standards. Side letters will be used to refine information rights and compliance clauses for public company and other strategic investors. As strategics and traditional fund and venture capital investors continue to pursue different exit timelines, expect to see new contractual tools – drag-along waivers and explicit exit alignment clauses – to manage potential misalignment.

Corporate venture capital now sits at the intersection of innovation, finance, and strategy. It allows established companies to stay agile in the face of technological disruption and gives startups credibility and market reach they could not achieve alone. For Canada, the continued growth of corporate venture capital represents an opportunity to build a stronger innovation economy and a more resilient venture capital ecosystem. Canadian corporates that invest thoughtfully – balancing strategy, governance and risk – will be the ones that help define the next generation of Canadian leaders in innovative companies.



Digital Infrastructure Investment in Canada

The digital infrastructure sector in Canada saw significant activity and investment in 2024 and 2025, with private equity investors driving a number of major M&A and greenfield transactions in data centres, fibre and wireless infrastructure, communications towers, and other digital assets. Global activity in the digital infrastructure sector is rapidly expanding with significant increases in demand for artificial intelligence, cloud storage, and other digital services – and Canada is no exception.[1]

Looking ahead to 2026 and beyond, digital infrastructure investment in Canada is expected to remain strong, supported by significant governmental support. The Government of Canada has highlighted "nation building" as a top priority and identifies digital infrastructure as a key driver of economic growth and innovation. Programs such as the Universal Broadband Fund[2] are supporting the expansion of high-speed internet access, including in rural and remote communities, while Prime Minister Mark Carney's commitment to developing AI infrastructure – the "Build AI" initiative[3] – aims to position Canada as a global leader in digital innovation. The Canada Infrastructure Bank is also playing a critical role, providing dedicated funding for large-scale digital projects, including fibre optic networks.[4]

Canada's leadership in artificial intelligence (which we highlighted in our **2025 Private Equity Outlook**) is further accelerating digital infrastructure investment in Canada, particularly in the data centre sector. Canada's AI ecosystem, anchored by hubs in Toronto, Montreal and Edmonton, has led to a surge in data centre projects.[5] Provincial governments in Canada are also supporting this trend with initiatives such as Ontario's Energy Plan[6] and Alberta's Artificial Intelligence Data Centres Strategy,[7] designed to attract further investment and foster innovation in data centres and AI. The acceleration of Canada's data centre sector is also resulting in significant expansion in energy storage and battery storage projects, which are necessary to ensure that data centres and other digital assets have access to reliable, sustainable power. The Canada Energy Regulator predicts that installed energy storage capacity in Canada may increase from 552MW at the end of 2024 to 1,149 MW in 2030, based solely on projects that are currently under construction.[8]

Another significant trend in 2025 has been the monetization of digital infrastructure assets by a number of major Canadian telecommunications companies, which have divested substantial stakes in non-core assets such as backhaul infrastructure and tower assets, to PE-backed investors and infrastructure funds. These transactions reflect a broader industry shift in Canada, as telecommunications providers focus on core services and balance sheet optimization.

The scale and complexity of deals in Canada have fostered a robust investment environment, with private equity investors collaborating with Canadian pension funds, global infrastructure investors, and strategics to tackle large, capital-intensive projects. Canada's financial and regulatory framework further enhances investor appetite for digital infrastructure in Canada. With strong market fundamentals, supportive government policy, and a deep pool of sophisticated investors, Canada's digital infrastructure sector is poised for continued growth. The convergence of digital and energy infrastructure, the rise of AI, and the ongoing build-out of broadband and wireless networks are creating opportunities for investment. As the sector evolves, Canada is well positioned to remain at the forefront of digital and energy infrastructure investment, offering scale, stability, and innovation.

1 MarketsandMarkets™, "***Cloud AI Market Size, Size, Growth & Latest Trends***" (Dec. 2024) and Goldman Sachs, "***AI to drive 165% increase in data center power demand by 2030***" (Feb.4, 2024).
2 Information, Science and Economic Development Canada (ISEDC), "***Universal Broadband Fund***" Government of Canada (2025).
3 Liberal Party of Canada, "***Canada Strong – Build***" Government of Canada (2025).
4 Canada Infrastructure Bank, "***Addressing Canada's Digital Divide – CIB Broadband Investments Surpass $2 billion***" (2025).
5 Kyle Bakx, "***Data centres are hungry for power, and Alberta is pitching itself as the place to build***" CBC News (August 18, 2024).
6 News.Ontario.ca, "***Ontario's energy plan unlocking opportunities in the digital economy***" Government of Ontario (July 2, 2025).
7 *Alberta.ca*, "***Artificial Intelligence Data Centres Strategy***" Government of Alberta (2025).
8 Canada Energy Regulator, "***Market Snapshot: Energy Storage in Canada may multiply by 2030***" Government of Canada (July 23, 2025).

Open Banking in Canada: The Journey, the Present, and the Emerging Road Ahead

Open banking, also known as consumer-driven banking, is a system that allows consumers and businesses to securely share their financial data with other third-party service providers. Several countries require financial institutions to make their customers' financial data available through a legislated open-banking regime. While such a regime does not currently exist in Canada, there has been a concerted effort by the federal government to implement such a regime in short order. If these efforts are successful and open banking becomes widely adopted by Canadian financial institutions, it would represent a major transformation in Canada's financial and payments landscape.

For organizations, open banking introduces a range of new opportunities and challenges. These include meeting new compliance requirements, adapting to evolving liability and cybersecurity standards and making strategic decisions related to data access, operational efficiency and risk management. As Canada's open-banking framework continues to mature, those organizations that proactively assess their readiness, update compliance processes and explore new business models will be best positioned to capitalize on the emerging opportunities.

THE JOURNEY SO FAR: HOW WE GOT HERE

Background and Motivations

For many years, Canadian consumers and businesses encountered significant challenges in sharing their financial data efficiently and securely. The absence of a standardized framework led to widespread reliance on "screen scraping," a practice through which users provide their confidential login credentials to third-party aggregators. This approach exposes sensitive information and creates liability and privacy risks, while also limiting the potential for innovation and consumer empowerment. In response to these challenges, the federal government initiated consultations and working groups to explore safer, more robust approaches to financial-data sharing. The overarching goal was to empower consumers, foster competition and support the growth of Canada's digital economy.

Key Milestones

Canada's path toward open banking has recently advanced through a series of policy and legislative milestones:

— **The federal *Budget 2024*:** The federal government formally announced plans to introduce a consumer-driven banking framework emphasizing safety, consumer protection and economic growth.

— ***Consumer-Driven Banking Act* ("CDBA"):** Part 1 of the CDBA received Royal Assent in June 2024, establishing a high-level legislative framework for open banking.



— **Political developments:** The prorogation of Parliament and a federal election in early 2025 delayed further implementation.

— ***Budget 2025* and Bill C-15:** In November 2025, the government introduced a revamped version of the CDBA as part of Bill C-15, signaling renewed momentum and accelerating legislative progress.

WHERE WE ARE NOW: THE CURRENT STATE OF OPEN BANKING

Legislative and Regulatory Landscape and the CDBA

The CDBA, as currently envisioned in Bill C-15, sets out a draft statutory foundation for open banking in Canada. As of the date of writing this article, Bill C-15 has passed second reading in the House of Commons and has been referred for consideration in committee. As such, the fate of the CDBA is uncertain, and there may be changes to the current language found in Bill C-15. The summary below is based on the language in Bill C-15 as of the date of writing this article – stay tuned to **McCarthy Tétrault's TechLex** for the updates as they happen.

Key Framework Elements

The CDBA open-banking framework applies to both individuals and businesses, and covers a wide range of financial products, including deposit accounts, investments, payment products and lending accounts. Notably, "derived data," which is data that has been enhanced to increase its usefulness or commercial value, is currently excluded from scope.

Phase 1 of implementation enables read-only access, allowing consumers to securely direct participating entities to access their financial data. The long-standing practice of screen scraping will be prohibited once the CDBA comes into force, which will reduce the liability and security risks associated with that practice. Oversight and implementation of the framework is entrusted to the Bank of Canada from the Financial Consumer Agency of Canada.

Participation in open banking will be mandatory for certain banks, based on prescribed retail-volume thresholds. Other financial institutions, payment-service providers and eligible entities may participate on a voluntary basis, subject to tailored accreditation requirements. This establishes common national rules governing privacy, consent, liability, cybersecurity, and national-security safeguards. Third-party service providers may support core functions such as consent management and authentication, but they must be accredited according to the requirements of the CDBA to do so.

Consumer Protections and Compliance

The new framework includes various consumer protections and compliance requirements. The CDBA states that consumers are not liable for financial losses resulting from authorized data sharing, except in cases of gross negligence. Details on redress and compensation processes will be clarified in future regulations.

Entities participating in open banking must obtain clear, simple and revocable consent from consumers, with regular reconfirmation and accessible dashboards. Both internal and external complaints processes are mandated, providing robust mechanisms for redress.

THE ROAD AHEAD: WHAT'S NEXT FOR OPEN BANKING

As outlined by the federal government in *Budget 2025*, Canada's approach to open banking will advance through a two-phase rollout. Phase 1, which is currently underway, focuses on read-only access and secure data sharing. Phase 2, targeted for mid-2027, will expand the framework to include write-access, enabling payment initiation and account switching. The rollout of Phase 2 is contingent on the implementation of Real-Time Rail payments infrastructure. This is an ambitious roadmap with very aggressive timelines, so organizations should prepare to act quickly (both to comply with the requirements applicable to them once they come into force and also to leverage the opportunities that the open-banking framework will open).

WHAT'S NEXT FOR YOU

As Bill C-15 and the CDBA move from concept to implementation, businesses should begin preparing for greater data mobility, enhanced security obligations and a more competitive financial-services landscape.

With Phase 1 already working its way towards becoming law, and Phase 2 on the horizon, staying informed about regulatory developments and legislative changes will be essential. Given the pace of change and the magnitude of details and requirements that are yet to be finalized, please follow **McCarthy Tétrault's TechLex** for the most recent updates regarding the CDBA and open banking in Canada.

Canada's Stablecoin Act: A Bold Step Forward

On November 18, 2025, the federal government published the *Stablecoin Act* (the "Act") as Division 45 of ***Bill C-15: An Act to implement certain provisions of the budget tabled in Parliament on November 4, 2025***. The Act establishes a registration framework for issuers of stablecoins – digital assets intended or designed to maintain a stable value relative to the value of one fiat currency – to be administered by the Bank of Canada ("BoC").

Publication of the Act is a landmark event for Canada's crypto asset industry, which has been lobbying the federal government for years to bring Canada into step with other jurisdictions that are regulating stablecoins as electronic money or payment instruments. Canada has been the only major economy attempting to regulate stablecoins as securities, using a disclosure-based framework ill-suited to address the safeguarding and liquidity risks associated with stablecoins. While the new legislation will not eliminate the potential characterization of stablecoins as securities, it should provide a path to licensure for issuers under a clear, prudentially oriented regime.

WHAT ARE STABLECOINS?

The term "stablecoin" is generally used to describe a digital asset that is recorded on a public, permissionless blockchain ledger that is intended to represent the value of a single fiat currency. While stablecoins were initially introduced as a tool for crypto asset trading and lending, in the past few years use cases for stablecoins for peer-to-peer payments, cross border remittance and institutional settlement have gained traction. As of February 19, 2026, the VISA Onchain Analytics Dashboard reported approximately US$6.5 billion of retail transaction volume and US$150.6 million of retail-sized transactions over the prior 30-day period.[1]

As a result, a range of global regulatory initiatives have emerged to address consumer protection risks associated with stablecoins, primarily by imposing prudential regulatory frameworks on stablecoin issuers, including reserve and redemption requirements, risk management programs, privacy and data protection considerations and interaction with anti-money laundering (AML), anti-terrorist financing (ATF) and economic sanctions regimes.

WHY DOES CANADA NEED STABLECOIN LEGISLATION?

It is not surprising that U.S. dollar-denominated stablecoins are globally dominant, with USD Tether (USDT, issued by Tether International, S.A. de C.V. based in El Salvador), USD Coin (USDC, issued by Circle Internet Group, Inc., conditionally approved by the U.S. Office of the Comptroller of the Currency (OCC) to establish a national trust bank) and various U.S. dollar stablecoins issued by Paxos Trust Company, N.A. (now regulated by the OCC) and its affiliates in the European Union (EU) and Singapore representing the vast majority of global stablecoin volumes. In July 2025, the U.S. government passed the *Guiding and Establishing National Innovation for U.S. Stablecoins Act* ("GENIUS Act"), accelerating stablecoin adoption in the United States. The



1 Visa Onchain Analytics Dashboard in collaboration with Allium Labs, ***Stablecoin Transactions.***



GENIUS Act followed implementation of the EU's Market in Crypto Assets (MiCA) regime in December 2024, which regulates stablecoins as "e-money tokens."

USD stablecoins have been widely used within the Canadian crypto asset markets for many years. Since the Canadian Securities Administrators (CSA) exerted jurisdiction over custodial crypto asset exchanges and brokers, commonly known as Crypto Trading Platforms ("CTPs"), in 2021, the CSA were first to identify consumer protection risks related to stablecoins. Absent any other existing or emerging Canadian regulatory regime to address these risks, the CSA sought to fill the void by regulating stablecoins as securities. This approach has deterred almost all USD stablecoin issuers from obtaining approval to offer their tokens in Canada and has also chilled attempts by potential Canadian stablecoin issuers to gain widespread adoption.

Following passage of the GENIUS Act in the United States, the federal Department of Finance recognized the need for a similar prudential framework in Canada and moved quickly to introduce legislation as part of *Budget 2025*. The Act sets high but attainable standards for issuers that are intended to protect Canadian users and should encourage the development and adoption of Canadian dollar-denominated stablecoins.

The *Stablecoin Act* sets out a high-level framework, with the expectation that further details will be prescribed in regulations to be developed in consultation with stakeholders following the adoption of the Act.

WHAT ARE THE KEY REQUIREMENTS FOR STABLECOIN ISSUERS?

Prior to creating a stablecoin and making it available for purchase, directly or indirectly, by a person in Canada, the issuer must register with the BoC by submitting an application which describes or includes the following:

- Ownership and organizational structure of the issuer
- Redemption policy pursuant to which each coin can be redeemed for one unit of the reference currency, at par value
- Composition of reserve assets, which must:
  - have a value equal to or greater than all outstanding coins, composed of the reference currency or other liquid assets denominated in the reference currency,
  - be unencumbered, segregated and bankruptcy remote,
  - be held with qualified custodians, and
  - be used for no purpose other than to fund redemptions
- Audited financial statements, including the number of outstanding coins, composition of reserve and sufficiency of reserve to fund redemptions
- Legal opinion regarding the issuer's compliance with the reserve requirements
- The issuer's enforcement history regarding anti-money laundering (AML)/anti-terrorist financing (ATF) regulation, market conduct and consumer protection matters
- Technical descriptions of the issuer's distributed ledgers, smart contracts, code and infrastructure
- The issuer's policies with respect to:
  - governance: roles and responsibilities, accountability and oversight, outsourcing and conflicts of interest;
  - risk management: resilience, incident response, business continuity, outsourcing, cybersecurity, and AML/ATF;
  - data security: personal information and data protection; and
  - recovery and resolution: orderly wind-down process.

For further details regarding the contents of the Act, check out our **December 4, 2025 presentation: Stablecoin Act: First Impressions**.

WHAT ARE THE KEY PROHIBITIONS AND RESTRICTIONS FOR STABLECOIN ISSUERS?

Stablecoin issuers are prohibited from directly or indirectly granting or paying to the holder of its coins any form of interest or yield, whether in cash, digital assets or otherwise. This prohibition is framed more broadly than a similar provision in the GENIUS Act; however, many U.S.-based financial institutions are pushing for similar breadth in the course of regulatory consultations. If interpreted broadly, this prohibition could restrict participants in stablecoin networks from the common practice of rewarding users for holding stablecoins on their platforms.

The Act stipulates that stablecoins are not legal tender, not deposits and not insured under a public or government system, and prohibits issuers from making representations to the contrary, including through the use of prohibited terms, expressions, logos or symbols to be prescribed by regulation.

The Act anticipates that prudential regulations and/or BoC guidelines will be made and empowers the BoC to make directions against issuers regarding unsafe and unsound practices.

Issuers must notify the BoC of significant changes, as well as any "incident" that is an unplanned event or series of events that results or could reasonably result in the reduction, breakdown or deterioration of activities performed by the issuer or a service provider related to the stablecoin.

HOW DOES THE *STABLECOIN ACT* INTERACT WITH OTHER CANADIAN REGULATORY REGIMES?

Federal AML/ATF Legislation

All stablecoin issuers are considered dealers in virtual currency and must register as money services businesses (MSBs) under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), resulting in shared oversight between the BoC and the Financial Transactions Reporting and Analysis Centre of Canada (FINTRAC).

Retail Payment Activities Act

The *Retail Payment Activities Act* (Canada (RPAA), also administered by the BoC, will be amended to add a new "payment function": the transmission or maintenance of an end user's encrypted or tokenized payment instrument or end user's private key, whether or not encrypted or tokenized. This amendment will clarify that payment service providers (PSPs) registered under the RPAA are permitted to use stablecoins when providing payment services to Canadian consumers and businesses.





Federally Regulated Financial Institutions

The *Stablecoin Act* does not apply to federally regulated financial institutions (FRFIs). A **federal government Policy Statement dated February 9, 2026** indicates that financial institution regulators, such as OSFI, will regulate the issuance of stablecoins by financial institutions under their jurisdiction.

Unlike the GENIUS Act, the *Stablecoin Act* does not expressly contemplate that FRFIs may establish subsidiaries to issue stablecoins in compliance with the Act, nor does it expressly prohibit such a structure.

Securities Legislation

The Act stipulates that issuing a compliant stablecoin is not dealing in securities under the federal *Bank Act*, *Insurance Companies Act* or *Loan and Trust Companies Act*. However, the Act is silent on the application of provincial securities legislation to stablecoin issuers, likely for jurisdictional reasons.

In a **September 2024 press release**, the CSA suggested that it was compelled to regulate value-referenced crypto assets as securities due to the lack of any Canadian initiatives to develop payment-based or banking-based regimes for stablecoins. However, at a Hearing of the Senate Standing Committee on Banking, Commerce and the Economy held on December 9, 2025, the Ontario Securities Commission (OSC) pushed for "hybrid" jurisdiction over stablecoin issuers to be exercised by a committee comprised of federal and provincial regulators. The OSC did not articulate any specific consumer protection concerns that could not be addressed sufficiently by a framework administered by the BoC, as contemplated in the Act.

The **federal government Policy Statement dated February 9, 2026** clarifies that the CSA will retain jurisdiction over stablecoins that are not fiat-backed, as well as the trading of stablecoins on crypto trading platforms. Further details and clarity will emerge as regulations are developed under the Act. We are optimistic that Canada's crypto asset sector, and the financial services industry more generally, will advocate for a streamlined regulatory approach which builds upon the bold first step taken by the federal government with the publication of the *Stablecoin Act*.

Navigating Canada's Evolving Payments Regulatory Landscape

Recent developments in Canada's payments regulatory space have come with exciting opportunities for innovation as well as significant compliance challenges for organizations. The end of 2025 was particularly eventful, with the remaining provisions of the *Retail Payment Activities Act* (Canada) ("RPAA") coming into force on September 8, 2025, and the introduction of the *Stablecoin Act* (Canada) ("SB Act") and revised *Consumer-Driven Banking Act* (Canada) ("CDBA") in the federal budget bill in November 2025. In addition, Payments Canada continued to make progress on the implementation of Canada's new payment rail, Real-Time Rail ("RTR").

RPAA: COMPLIANCE REQUIREMENTS

The provisions of the RPAA that came into effect on September 8, 2025 imposed substantial compliance requirements on payment service providers ("PSPs"). Throughout the months leading up to the effective date of these provisions, PSPs engaged in readiness activities, which required substantial efforts by many PSPs to prepare to comply with obligations related to safeguarding end-user funds, operational risk and incident response, and reporting and record keeping, among others. The broad scope of the RPAA, the activities it applies to, and the rigour of the compliance obligations it imposes were unexpected for many organizations, particularly foreign organizations that provide PSP services to Canadian clients but are not otherwise subject to a comparable regime in their home jurisdiction.

While the Bank of Canada has not yet issued any administrative monetary penalties to PSPs for RPAA violations, they have been contacting organizations that have not yet registered as a PSP but that the Bank of Canada views may be subject to the RPAA. The Bank of Canada has also been engaging with those PSPs that have registered, or have applied for registration, with questions or to discuss the compliance obligations under the RPAA. At this time, the Bank of Canada's approach has been to encourage compliance with the RPAA, but 2026 may see the first enforcement actions taken by the Bank of Canada under this regime.

It will also be interesting to see if there is additional scrutiny by the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") of those organizations that registered with the Bank of Canada as a PSP but are not registered with FINTRAC as a money services business ("MSB") or foreign MSB under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (Canada) ("PCMLTFA"), and vice versa, given there is significant overlap of the criteria requiring registration under both regimes.

REAL-TIME RAIL AND CONSUMER-DRIVEN BANKING (OPEN BANKING)

The federal budget released in November 2025 (*Budget 2025*) highlighted the intention for phase two of the CDBA to be in effect by mid-2027, which would allow for broader functionality (write-access to consumer data) and expanded participant scope, and aligns with the intention for RTR to be in widespread use





by this time. Together, RTR and consumer-driven banking have the potential to greatly expand payment solutions, including enabling new ways for Canadians to initiate data-rich, real-time payments directly from their bank account, as well as other potential use cases.

However, for fintechs in particular, participation in RTR and consumer-driven banking will be far from simple, as the requirements of multiple regulatory regimes must be met, including:

- successfully registering as a PSP with the Bank of Canada under the RPAA,
- successfully registering as an MSB or foreign MSB with FINTRAC under the PCMLTFA (likely required given the nature of activities to be conducted),
- becoming a member of Payments Canada,
- being accepted as a participant in RTR (which includes technical, testing and other requirements),
- being approved by the Bank of Canada for an RTR settlement account, and
- meeting the accreditation requirements required under the CDBA.

The foregoing list of requirements illustrates that embracing innovation and being successful in the payments space in Canada will increasingly demand not only technological sophistication but also robust regulatory and compliance frameworks and expertise.

EXPANDED OVERSIGHT AND ENFORCEMENT

Over the last few years, the Bank of Canada's role has continued to grow beyond directing monetary policy and currency issuance to exercising supervisory authority over PSPs under the RPAA, and in the future, over those organizations that become subject to the SB Act and the CDBA. This expanded role of the Bank of Canada aligns with its mandate to promote a safe and efficient financial system.

FINTRAC's oversight role has also expanded to include additional organizations such as those providing acquirer services in relation to private ABMs, cheque cashers, factors, financing and leasing entities, and title insurers. Recent legislative proposals aim to increase penalties for violations of the PCMLTFA and its regulations up to a maximum of C$20 million per occurrence or 3% of a reporting entity's gross global revenue. This, combined with recent enforcement activity and significant fines under the current provisions of the PCMLTFA, emphasizes the criticality of compliance, particularly for MSBs (and foreign MSBs).

Budget 2025 also proposed to establish a new financial crimes agency as the lead and centralized federal enforcement agency, as well as additional amendments

to the PCMLTFA, including restrictions on large cash transactions and third-party cash deposits. FINTRAC is also proposed to be added as a member of the Financial Institutions Supervisory Committee, which would enable greater oversight and coordination with prudential regulators.

SUCCESS AMIDST REGULATORY CHANGE

To successfully navigate the rapid pace of change in payments regulation, businesses must be proactive and take a number of steps, including:

- monitoring regulatory developments closely and maintaining an updated repository of applicable laws and regulations;
- developing a plan to ensure compliance by required timelines, as drafting and implementing required policies, procedures, training and compliance programs is complex and it can take substantial time and resources to develop, review and obtain required approvals; and
- retaining legal and compliance advisors early in strategic planning and business initiatives to assist with preventing surprises, appropriately managing risk, and avoiding unexpected regulatory delays later in the process.

Canada's payments ecosystem continues to evolve. The outlook for 2026 and beyond shows great momentum for innovation if regulation continues to keep pace and strikes the appropriate balance of ensuring the safety and soundness of Canada's payment systems and the protection of Canadians without imposing an excessive regulatory burden on those pursuing the realization of the future of payments in Canada. Organizations that can adapt, anticipate regulatory changes and invest in compliance readiness will be well positioned to navigate this dynamic environment.



Hot Topics in Privacy and Cybersecurity

The past year included several notable moments in Canadian privacy and cybersecurity law. Regulatory authorities have demonstrated a willingness to take bold action, courts have issued precedent-setting decisions, and Parliament has debated broad legislative reforms that will shape the future of technology regulation.

RECENT DECISIONS AND REGULATORY GUIDANCE

The regulatory environment for technology businesses operating in Canada has grown increasingly complex, as demonstrated by several high-profile investigations and decisions.

i. TikTok: Consent and Age Verification Mechanisms

In September 2025, the Privacy Commissioner of Canada, together with provincial counterparts from Québec, Alberta, and British Columbia, released their **findings of their joint investigation** that scrutinized TikTok's privacy practices.[1] The Commissioners ultimately held that the platform's approach to age assurance, consent, and privacy by default were inadequate.

According to the Commissioners, TikTok's systems failed to reliably prevent children under the age of thirteen (fourteen in Québec) from accessing the platform, resulting in the collection of personal information for inappropriate purposes. In addition, they found that the platform did not provide sufficient clear, upfront information at the time of account creation, especially for youth, and that TikTok's privacy policy and educational tools were not considered sufficiently comprehensible. Explanations of target advertising, content personalization, and biometric information use were found to be inadequate. Furthermore, the Commissioners found that TikTok did not default to the most privacy protective settings, in violation of Québec's privacy-by-default provisions.

As a result, the Commissioners recommended that TikTok conduct rigorous privacy impact assessments, and that it implement enhanced age-gating mechanisms, comprehensive privacy-by-default functions, and upfront disclosures about cross-border data flows. TikTok responded by agreeing to implement three age assurance mechanisms, refreshing privacy disclosures, ceasing targeted advertising to minors except by generic categories (e.g., language and approximate location), and launching a centralized "Privacy Settings Check-up" for Canadian users. These steps led regulators to conclude that the matter was "well founded and conditionally resolved." Nevertheless, lingering questions remain regarding the legal standard for compliance, the fate of improperly collected data, and the possibility of judicial review. The TikTok case illustrates the growing expectations for transparency, accountability, and privacy protection in digital platforms, especially those with large youth audiences.



1 *PIPEDA Findings #2025-003: Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta - Office of the Privacy Commissioner of Canada.*

ii. Google: Right to be Forgotten

A **landmark case involving Google** addressed whether search engines must delist prejudicial articles under Canada's ***Personal Information Protection and Electronic Documents Act* (PIPEDA)**.[2] The complainant argued that outdated, misleading, and harmful articles should be removed from search results. After years of jurisdictional disputes, the Office of the Privacy Commissioner established a balancing test, clarifying that delisting is appropriate only when significant harm to the individual outweighs the public interest in access to information. Notably, Google was not required to verify the accuracy of underlying news articles. This decision sets important boundaries for the "right to be forgotten" in Canada, emphasizing the need to balance privacy rights with freedom of expression and public access to information. The Google case is likely to influence future disputes involving online reputation, search engine liability, and the scope of privacy rights in the digital age.

iii. Clearview AI: *Charter* Challenge

Clearview AI, a US-based facial recognition company, was investigated for scraping billions of images from social media and other public sources.[3] Alberta's privacy regulator **ordered** Clearview AI to cease operations and stop collecting images from Albertans, and Clearview AI subsequently challenged the order, arguing that consent requirements infringed its freedom of expression under the Charter.[4] The Alberta court broadened the publicly available exception to include social media, but **maintained** that Clearview AI's mass scraping for commercial surveillance was not a reasonable purpose under privacy law.[5] The court rejected Clearview 's argument that technical inability to comply excused non-compliance, reinforcing the enforceability of privacy orders. This case highlights the tension between technological innovation and privacy protection, with courts affirming robust enforcement powers for regulators. The Clearview AI decision also signals that Canadian courts are prepared to scrutinize the purposes and methods of data collection, especially when mass surveillance and biometric technologies are involved.

iv. *ICBC v. Ari: Privacy Act* Damages in the Absence of Proof of Loss

In British Columbia, an Insurance Corporation of British Columbia (ICBC) employee accessed and sold private information of policyholders, with several victims' data sold to criminals, resulting in privacy breaches and subsequent criminal acts.[6] In ***ICBC v. Ari***, the affected policyholders sued ICBC in a class action.[7] Section 1 of the ***Privacy Act*** creates a tort actionable without proof of harm for willful privacy violations.[8] The court upheld an award of $15,000 per class member in general damages, emphasizing that serious privacy breaches justify substantial symbolic damages, even without proof of consequential harm.[9] This precedent is likely to increase the volume of privacy class actions in BC, especially in cases involving egregious facts or vicarious liability. The *ICBC v. Ari* case demonstrates that Canadian courts are willing to impose significant financial consequences for privacy violations, even in the absence of quantifiable harm, thereby reinforcing the importance of robust privacy compliance programs.

RECENT LEGISLATIVE DEVELOPMENTS

i. Federal Commitment to Technology Leadership

In 2025, Canada appointed its first **Minister of Artificial Intelligence**, signaling a commitment to technology leadership and innovation.[10] However, privacy remains absent from the federal mandate letter and platform, raising questions about the future of comprehensive privacy and AI legislation. Despite this uncertainty, however, the government's focus includes protecting children's personal information, combating deepfakes, and promoting Canadian digital sovereignty. **Initiatives** such as the AI Strategy Task Force and plans for sovereign cloud computing capabilities also reflect a broader push for digital infrastructure and data sovereignty.[11] Legal professionals will be monitoring these developments closely, as future legislation may reshape regulatory

2 ***PIPEDA Findings #2025-002: Investigation and recommendations concerning Google search engine service's compliance with its obligations under PIPEDA - Office of the Privacy Commissioner of Canada***.
3 ***https://www.mccarthy.ca/en/insights/blogs/techlex/court-kings-bench-alberta-strikes-provisions-pipa-unconstitutionality***
4 Clearview AI Inc. v Information and Privacy Commissioner for British Columbia, 2024 BCSC 2311 (CanLII), <***https://canlii.ca/t/k8fq2***>.
5 Clearview AI Inc v Alberta (Information and Privacy Commissioner), 2025 ABKB 287 (CanLII), <***https://canlii.ca/t/kc1r5***>.
6 ***https://www.mccarthy.ca/en/insights/blogs/canadian-class-actions-monitor/bc-court-appeal-confirms-privacy-act-damages-may-be-awarded-without-proof-loss***
7 Ibid.
8 ***https://laws-lois.justice.gc.ca/eng/acts/p-21/FullText.html***
9 Insurance Corporation of British Columbia v. Ari, 2025 BCCA 131 (CanLII), <***https://canlii.ca/t/kbnrq***>
10 ***https://www.cbc.ca/news/politics/artificial-intelligence-evan-solomon-1.7536218***
11 ***https://www.canada.ca/en/innovation-science-economic-development/news/2025/09/ministers-joly-and-solomon-meet-the-future-of-ai-at-all-in-2025.html***

compliance obligations and cross-border data flows.

ii. Bill C-8: Critical Cyber Systems Protection Act

Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts introduces significant amendments to the *Telecommunications Act* and establishes new cybersecurity obligations for designated operators in vital sectors and systems.[12] Organizations must develop and maintain cybersecurity programs, as well as regularly assess and manage cyber risk, including supply chain vulnerabilities. Material changes in third-party providers must be reported, and all cybersecurity records must be stored within Canada. Canadian regulators gain broad powers to audit, enter premises, and issue binding orders. Fines can reach $15 million per violation per day for organizations, with personal liability for directors and officers if such persons were complicit in committing violations. Sector-specific oversight is delegated to various regulators, including the Office of the Superintendent of Financial Institutions for banking systems, the Bank of Canada for clearing and settlement systems, the Canadian Energy Regulator for pipelines and power lines, the Canadian Nuclear Safety Commission for nuclear energy, the Minister of Industry for telecommunications, and the Minister of Transport for transportation systems with federal jurisdiction.

The scope of Bill C-8 is broad, affecting telecommunications, energy, transportation, banking, and clearing systems. Organizations operating in these sectors must conduct readiness assessments, review vendor risk management, develop internal compliance processes, and monitor legislative progress to anticipate compliance timelines. The risk of substantial fines and personal liability for directors and officers underscores the need for proactive preparation. Bill C-8 also reflects international trends, drawing inspiration from cybersecurity frameworks in Australia, the European Union, the United Kingdom, and the United States.

In addition to Bill C-8, ***Bill C-12, Understanding Strengthening Canada's Immigration System and Borders Act*** revisits earlier proposals to expand police and Canada Post authority to search mail and facilitate access to telecommunications data.[13] While "lawful access" provisions have been excised for now, they are expected to resurface in future legislation, reflecting ongoing debates about privacy, surveillance, and law enforcement powers. The evolution of lawful access provisions will be closely watched by privacy advocates, law enforcement agencies, and technology companies alike.

PRACTICAL GUIDANCE FOR BUSINESSES

2025 has been an activity-filled year for Canadian privacy and cybersecurity law and regulation. High-profile enforcement actions, judicial decisions, and ambitious legislative proposals continue to reshape the legal landscape, presenting both challenges and opportunities for businesses. Given the evolving regulatory and legislative landscape in Canada, businesses must remain vigilant and adaptable. It is essential to monitor regulatory decisions, court cases, and legislative developments affecting privacy and cybersecurity. 2025 has emphasized that regular privacy and cybersecurity assessments should be conducted, with a focus on age assurance, consent mechanisms, and privacy-by-default settings. Transparency in data collection, use, and cross-border flow is crucial, and businesses should ensure clear disclosures and robust consent processes. Internal processes for reporting, record-keeping, and responding to regulatory audits or investigations must be developed and maintained. Engaging legal counsel is advisable, especially in areas involving AI, biometric information, and cross-jurisdictional compliance.

Businesses should also pay close attention to the potential for increased enforcement activity, class actions, and reputational risks associated with privacy breaches. As Canadian law continues to evolve, businesses should be prepared to adapt their compliance programs, update their policies, and invest in privacy and cybersecurity training for personnel at all levels.

As Canada seeks to balance innovation, privacy, and cybersecurity, legal professionals play a crucial role in guiding clients through the complexities of technology law. Vigilance, adaptability, and proactive compliance will be essential for success in the year ahead.

12 ***https://www.parl.ca/LegisInfo/en/bill/45-1/c-8***
13 ***https://www.canada.ca/en/services/defence/securingborder/strengthen-border-security/understanding-stregthening-canada-immigration-system-borders-act.html***

Trends in AI Litigation: Lessons for 2026

Over the past year, artificial intelligence (AI) has moved well beyond early adopters and pilot programs to achieve deep integration in core business processes across industries. With increasing sophistication and utility, AI has transformed industries of all kinds and created opportunities that were unimaginable even just a year ago. At the same time, it has raised new and complex legal issues that courts in Canada and elsewhere have yet to resolve.

Looking ahead, 2026 is a pivotal moment for AI litigation. AI litigation is no longer hypothetical: it has arrived. But regulatory and common law frameworks are still taking shape. This chapter highlights the major trends emerging from the early stages of AI litigation in Canada and the U.S.

COPYRIGHT CLASS ACTIONS

The first wave of AI litigation in Canada and the U.S. has been dominated by proposed class actions alleging copyright infringement. These actions centre on how AI systems are trained and what they produce. Training modern large language models (LLMs) requires vast quantities of data. Plaintiffs have alleged that copyrighted materials were used to train certain LLMs by businesses that have not obtained licensing or proper permissions, and some plaintiffs have also alleged that outputs can replicate protected works.

Despite remaining in the preliminary stages, the proposed copyright class actions have already illustrated the high-stakes nature of AI litigation. For example, these proposed class actions seek damages on behalf of an extraordinarily broad and diverse class, including statutory damages under the *Copyright Act* up to $20,000 per work.

Canadian courts are now grappling with jurisdictional challenges as a preliminary issue. In late 2025, the Ontario Superior Court of Justice ruled that copyright claims brought by the *Toronto Star* and other newspaper publishers against OpenAI can be heard in Ontario.[1] That decision is under appeal. Given how central data is to AI development and these cases, copyright claims are expected to see significant developments and remain a leading area of AI litigation activity in 2026.

MISREPRESENTATION CLAIMS

Misrepresentation claims may be of interest to businesses that employ AI systems in their interactions with the public or customers. Generally, such claims allege that AI-enhanced services or systems provided false or misleading information due to the defendant's negligence, resulting in some loss to the plaintiff. These AI-enhanced services or systems may include customer service chatbots, automated support agents, and other tools that provide information.

Many questions about who bears responsibility for the outputs of AI and under what circumstances remain unresolved. Plaintiffs have alleged that businesses should be responsible for inaccurate or misleading statements produced by



1 Superior Court of Justice, "***Toronto Star Newspapers Limited v. OpenAI Inc., 2025 ONSC 6217***" CanLII (November 7, 2025).

their automated systems. Early decisions suggest that the nature of the technology may be less important than whether a company took reasonable steps to ensure the accuracy of the information it presents.[2]

REPUTATION, IMAGE AND PERSONALITY CLAIMS

AI systems can create content that affects or implicates the reputation, likeness or identity of real individuals. These claims in tort fall into three broad categories: defamatory statements, false light through synthetic media, and unauthorized use of an individual's voice or likeness:

- **Defamation**: Claims allege that AI has generated defamatory statements about individuals – for example, by falsely attributing harmful conduct to a person. Both warnings of inaccuracy and the growing public awareness that AI can make errors and "hallucinate" are considerations in alleged AI defamation claims.[3]
- **False light:** Courts are beginning to consider claims based on the creation or distribution of fabricated images or videos that place a person in an untrue and potentially offensive light. As AI tools improve and become more accessible, these disputes over content, often known as "deepfakes," are expected to grow.
- **Misappropriation of personality:** The unauthorized use of a person's voice, likeness or personality in AI-generated content is also garnering attention. This applies to the use of content that resembles a real individual without their consent for commercial purposes, including in marketing materials or promotional content.

PRODUCT LIABILITY

AI will continue to transform consumer markets. As AI systems are increasingly integrated into consumer products and services, from software applications to vehicles and home devices, AI-related product liability claims are expected to grow. But questions remain about how Canada's existing common law frameworks may apply to product liability claims relating to alleged harms involving failures in design, testing, or warnings associated with AI-enabled features. These frameworks will need to account for the ever-evolving nature of AI.

COMPETITION AND PRICING

AI-powered pricing tools are also attracting legal and regulatory attention. Automated pricing systems, especially those used in competitive markets, may influence prices across an industry in ways that allegedly resemble coordinated behaviour. Regulators in several jurisdictions have begun examining whether algorithmic pricing tools facilitate conduct that would otherwise be unlawful if carried out by direct communication among competitors.

The Competition Bureau is likely to continue to investigate the impacts of algorithmic pricing tools in markets such as fuel distribution, rentals and hospitality. These developments reflect broader concerns about transparency, fairness and the impact of automated decision making on consumers. Organizations using AI-enabled pricing tools should be evaluating how those systems work, the source of the data that they rely on, and whether their outputs could create the appearance of coordinated pricing.

A SHIFTING REGULATORY LANDSCAPE

The regulatory environment continues to evolve. Earlier attempts at a national AI statute were interrupted by the 2025 federal election, but renewed consultations indicate progress toward a new framework. Businesses should expect that any AI regulations in Canada will focus mainly on AI systems that have significant impact on individuals or markets, with possible requirements related to governance, risk assessment, documentation, and incident reporting.

OUTLOOK ON AI LITIGATION

AI offers transformative potential in a range of business sectors and raises new legal issues that courts are grappling with for the first time. While AI litigation in Canada remains in its infancy, it is poised to grow over the coming years. As that growth continues, we will continue to provide guidance and insights on how your business can navigate this evolving landscape with confidence.

2 Civil Resolution Tribunal of British Columbia, "***Moffatt v. Air Canada,* 2024 BCCRT 149**" CanLII (February 14, 2024).

3 Superior Court of Gwinnett County, State of Georgia, "***Walters v OpenAI LLC*, No. 23-A-04860-2**" ThomsonReuters.com (May 19, 2025).

Getting "IT" Right the First Time: How Early Decisions Determine the Success of Technology Projects

Most technology projects begin with optimism. Both vendors and customers have good reason to be excited by the opportunity to modernize processes, introduce new capabilities and build partnerships around technology solutions that are typically expected to deliver greater efficiency, better insights and improved experiences. Yet the most persistent challenges in technology projects can often be traced back to the decisions that are made amidst the optimism of the first few weeks or months of planning.

Technology projects are inherently complex. They typically involve many stakeholders, complicated technical requirements, lots of interdependencies and significant operational transformation. A lot can go wrong. Industry research shows that most technology projects fall short of expectations. Only 30% of organizations meet their timeline, budget and scope expectations when implementing major technology projects.[1] The other 70% fail, meaning they fail entirely or face costly overruns, delays or significant scaleback of core functionality. Businesses can avoid joining this majority by investing in the initial stages of a transaction. This chapter explores why early choices carry such weight, the recurring patterns that undermine projects and the practical steps businesses can take now to strengthen their next technology project.

HOW PROJECTS DRIFT BEFORE THEY BEGIN

The consequences of overlooking early warning signs are highlighted by the Government of Canada's troubled experience with the Phoenix Pay System project. The system exceeded its budget by more than 13 times, eventually costing the federal government close to C$4 billion. The Government of Canada set itself up for an overrun and overall failure by initially prioritizing budget minimization over solution objectives and pushing an aggressive timeline without appropriate contingency plans. Additionally, the project underestimated the complexity of government pay rules, relied on flawed assumptions in its business case, and lacked independent oversight. Many of these causes were visible at the outset, but by the time issues became undeniable, options were limited and expensive. As of late 2025, the federal government continues to deal with significant problems arising from this failed project, which launched in 2016.[2]

Common initial problems include:

— **Insufficiently clear objectives**: Without adequately defining the objectives for a technology solution and its initial requirements to support achievement of those objectives, the project team will not have a clear enough picture of the end state to be achieved. This often leads to misunderstandings, such as misinterpretation of requirements, and



1 Michael Grebe, et al., "***Most Large-Scale Tech Programs Fail—Here's How to Succeed***" Boston Consulting Group (November 13, 2024).

2 Campbell MacDiarmid, ***"Government demanding public servants reimburse years-old Phoenix overpayments"*** *CBC News* (November 28, 2025).

difficulties in making smart decisions when tough trade-offs are required as a project progresses.

- **Unrealistic timelines**: Technology initiatives can falter early on when working to unachievable timelines that are not grounded in how the organization works. Teams often underestimate the time required for internal approvals, privacy reviews, security assessments and stakeholder input. As the project progresses, those rushed assumptions resurface and create unintended consequences. The schedule tightens, quality pressures increase and previously manageable design choices begin to feel like compromises.
- **Poorly defined roles**: Ambiguity in roles and decision rights allows a deal to quickly slip away from its intended outcomes. When responsibilities are not clearly defined, stakeholders unintentionally shape the project without realizing it. A comment from a senior executive can be interpreted as an unwavering directive, or approval from a business unit treated as a high-level sign-off. If organizations do not firmly take control over the decisions that are important to them, their vendors may make uninformed and misaligned decisions on their behalf. Without clarity about who decides what, teams attempt to satisfy all voices. This usually results in rework, expanded scope or inconsistent direction.
- **Inefficient resource management**: Many organizations underestimate the depth of expertise needed to manage modern technology programs. Architectural decisions, integration planning and governance often require experienced contributors who are difficult to secure or too thinly spread across multiple initiatives. For example, if the staff turnover rate is high or pricing does not reflect the level of effort required, vendors may staff the project with smaller teams or less-experienced personnel, creating pressure points that emerge early and persist.
- **Delayed structure**: When early structures – such as the contract, solution requirements and governance processes – are weak, important foundational details and decisions are often deferred and governance becomes inconsistent. Decisions are made informally, documentation trails go missing, and temporary fixes are introduced to keep momentum, even if they obscure underlying issues. These patterns may seem harmless during the early planning stage, but they create conditions in which complex problems can take root.

STRUCTURING PROJECTS FOR SUCCESS

The organizations that effectively navigate technology projects share a common approach to the earliest stages of planning – they begin by finding mutual clarity. Their top priority is aligning on a shared understanding of the problem to be solved and the outcome they need the technology to deliver. This common understanding anchors subsequent decisions, especially when complexities or competing priorities are revealed in discovery or implementation stages.

Clarity naturally evolves into structure. Strong early planning includes thoughtful vendor engagement, where both sides communicate honestly and understand each other's constraints. These conversations lay the groundwork for a collaborative relationship rather than an adversarial one. Vendors who have a realistic view of their customer's internal processes and organizational dynamics can better design solutions that work. Customers who understand vendor resourcing realities can calibrate demands and avoid unrealistic assumptions.

Effective governance in the early stages is not about unnecessary frequent meetings or rigid oversight. It is about enabling timely, informed decisions. The best governance structures assign responsibility without overburdening any single group. They create predictable spaces for escalation and ensure that decisions made early are preserved throughout the project.

Strong governance also allows the parties to prepare to respond effectively to changes, instead of relying on the hope that nothing in the contractual environment will shift. As projects evolve over time, new risks and opportunities inevitably emerge. Governance frameworks that are adaptable rather than static help organizations navigate these shifts and achieve stronger outcomes.

Successful projects typically have well-defined milestones – not as mere administrative checkpoints but as opportunities for evaluation and reflection. Milestones with clear achievement criteria give teams an opportunity to pause, assess and realign if needed. They provide shared indicators of progress and help prevent misalignment between the contract and the lived experience of the project.

Procurement as a Strategic Stage

Procurement is often viewed as the administrative precursor to the "real" work of implementation. In practice, procurement is one of the most strategic stages of a

technology project, because it is the first point at which the project's vision is articulated and becomes concrete.

Strong procurement begins with internal diligence. Before engaging vendors, successful organizations ensure they understand their own requirements, including regulatory obligations, privacy considerations and existing contractual commitments. These insights form the basis of accurate, realistic procurement documents. When organizations skip this work, vendors respond to incomplete or ambiguous requirements, and miscommunication begins early.

The market diligence that follows is equally important. Understanding the vendor landscape helps organizations evaluate capabilities and make informed comparisons and provides a realistic sense of what the market can and cannot provide.

Contracting as a Blueprint for Collaboration

The contract that follows procurement is more than a collection of legal provisions. It is a blueprint for how the parties will work together. The most effective contracts balance clarity, protection and practicality. They allocate responsibilities, communicate expectations and establish the mechanisms that will keep the project aligned when complexity increases. Consider the following to ensure the contract can support your project throughout all stages:

- Clearly articulate roles, responsibilities, deliverables and processes to reduce friction, avoid confusion during delivery and support stronger collaboration.
- Ensure that the pricing model is sufficiently tied to successful outcomes and reflects the project's complexity and risks. Misaligned pricing creates pressure on staffing and quality, and it can distort incentives.
- Provide the necessary attention to termination rights, scope management and quality assurance provisions, as they protect both parties and ensure that the project can move forward even when challenges arise. Termination rights provide a way out if the parties have issues they cannot resolve, while quality provisions foster ongoing transparency and promote trust by giving both sides confidence in how progress will be continually evaluated and rewarded.

Delivering from a Strong Foundation

When delivery begins, the real value of early structure implementation becomes visible. Adequate staffing, clear governance and realistic expectations enable teams to manage technical complexity while staying aligned with strategic objectives. Steering committees keep direction consistent, documentation preserves continuity and escalation pathways ensure issues do not linger unnoticed.

No technology project is free from challenges. Integration issues, data questions and unexpected dependencies are inevitable. The difference between a successful project and a struggling one is not the absence of obstacles but the ability to address them quickly and constructively. Early discipline gives teams the structure and stability to resolve issues and avoid elevated levels of conflict and unintended consequences.

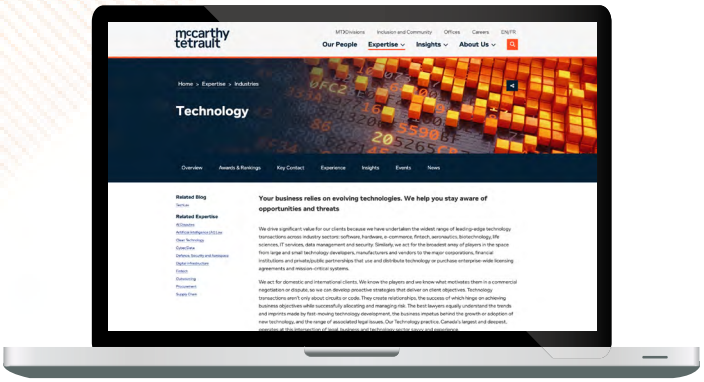
LESSONS FOR YOUR 2026 TECHNOLOGY PROJECTS

Organizations preparing for new technology initiatives can position themselves for success by focusing on a few core principles:

- Establish clarity about objectives and decision making before involving vendors.
- Invest early in internal expertise and external support where needed.
- Build governance supported by fit-for-purpose contractual frameworks that enables effective decision making and problem solving to save time and avoid disruption at critical times.
- Be intentional in the early stages of procurement and contracting to create transparency and alignment grounded in a strong understanding of the market and technology landscape.
- Remain willing to revisit assumptions and risk assessments as the project evolves.

While early discipline does not guarantee a perfect implementation, it creates the most favourable conditions for stable decision making, effective collaboration and predictable outcomes. When organizations invest in clarity, governance and early, thoughtful planning, they build a foundation strong enough to support the inevitable complexities of technology transformation. This strong start is often the difference between a project that stumbles and one that delivers lasting value.

VISIT OUR McCARTHY TETRAULT TECHLEX BLOG: TECHLEX | McCARTHY TÉTRAULT



> **"The client service is excellent - they are there when you need them with a quick response, and are very thorough and very knowledgeable of their subject matter."**
>
> — CHAMBERS GLOBAL, CLIENT INTERVIEW (TECHNOLOGY)

About McCarthy Tétrault's Technology Industry Group

McCarthy Tétrault's Technology Industry Group is the largest and deepest in any Canadian law firm. Operating at the intersection of the legal, business and technology sectors, our internationally recognized team of skilled advisors helps clients establish and maintain their competitive advantage. Our clients turn to us for our cross-functional legal expertise. We are technology industry experts first, with best-in-class transactional experience, which enables us to provide both day-to-day support on technology-related issues and industry-specific M&A counsel. Whether you are looking to grow via acquisition or to position your company to sell, our team will work with you to offer scaled, cost-efficient services and practical solutions that complement your goals. Among Canadian law firms, we've advised on the widest range of leading-edge technology transactions across industry sectors: software, hardware, e-commerce, fintech, aeronautics, biotechnology, life sciences, IT services, data management and security. Find out how our national, multi-disciplinary team can help you today.

About McCarthy Tétrault

McCarthy Tétrault LLP provides a broad range of legal services, providing strategic and industry-focused advice and solutions for Canadian and international interests. The firm has substantial presence in Canada's major commercial centres as well as in New York and London.

Built on an integrated approach to the practice of law and delivery of innovative client services, the firm brings its legal talent, industry insight and practice experience to help clients achieve the results that are important to them.

For further information on McCarthy Tétrault or any of the above, please contact **media@mccarthy.ca**

mccarthy tétrault

VANCOUVER
Suite 2400, 745 Thurlow Street
Vancouver, BC V6E 0C5

CALGARY
Suite 4000, 421 7th Avenue SW
Calgary, AB T2P 4K9

TORONTO
Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto, ON M5K 1E6

MONTRÉAL
Suite MZ400
1000 De La Gauchetière Street West
Montréal, QC H3B 0A2

QUÉBEC CITY
500, Grande Allée Est, 9e étage
Québec, QC G1R 2J7

NEW YORK
55 West 46th Street, Suite 2804
New York, New York 10036
United States of America

LONDON
1 Angel Court, 18th Floor
London EC2R 7HJ
United Kingdom