mccarthy tetrault

Technology Perspectives Outlook

2024

mccarthy tetrault

The Technology Industry Group at McCarthy Tétrault is pleased to present this Outlook publication on legal developments affecting the Canadian technology industry. This publication provides a timely and informative overview of some of the most noteworthy developments in 2023 and our outlook for 2024, from the perspective of our multi-disciplinary Technology Industry Group.

This publication is organized into two parts:

- **Part I** — Trends that are relevant to Canadian tech companies in the day-to-day operation of their business: **cybersecurity, privacy** and **immigration/global mobility**.
- **Part II** — Trends that are relevant to tech companies and their investors exploring financing or exit options, **particularly venture capital**, **bank financing** and **M&A**.

Part I: Day-to-day Considerations For Tech Companies

CYBERSECURITY UPDATE AND OUTLOOK

In the world of cybersecurity, the two main threats to companies remain: (i) business email compromise; and (ii) ransom-based attacks. Authorities expect ransomware to remain the most disruptive and persistent threat through 2024.[1] Data extortion, an attack where data is stolen and ransomed back to the owner, will also persist, often as part of a ransomware attack. While less high-profile than ransomware, business email compromise continues to be a significant source of economic loss and disruption for businesses.

The trend towards cloud migration, although mitigating ransomware risks, is creating more exposure for other attacks, such as data extortion. According to CrowdStrike, cloud exploitation cases grew by 95% and the number of cloud-conscious threat actors tripled.[2] Given this trajectory, threat actors are expected to continue adapting their operations to be compatible with cloud environments. Further, cyber threat actors are increasingly attacking organizations indirectly through software tools and services by exploiting supply chain compromises. This poses a significant threat where the vendor has access to the clients' networks.[3]

Changes to Canadian privacy legislation — including mandatory breach reporting and large fines in Québec, as well as the potential for fines federally — make cybersecurity incidents more expensive to deal with, resulting in increased financial risk to businesses. As a result, cybersecurity considerations continue to grow in importance in the context of M&A transactions.

DEVELOPMENTS IN CANADIAN PRIVACY LAW

The landscape for privacy and data protection laws in Canada is changing rapidly. New and reformed legislation is being discussed and proposed at various levels of government, including by the federal government and in several provinces. Courts are also making significant decisions that are further changing or clarifying the state of the law. Some of the more significant developments in this area from the past year occurred legislatively at the Canadian federal level and in Québec, and through new case law.

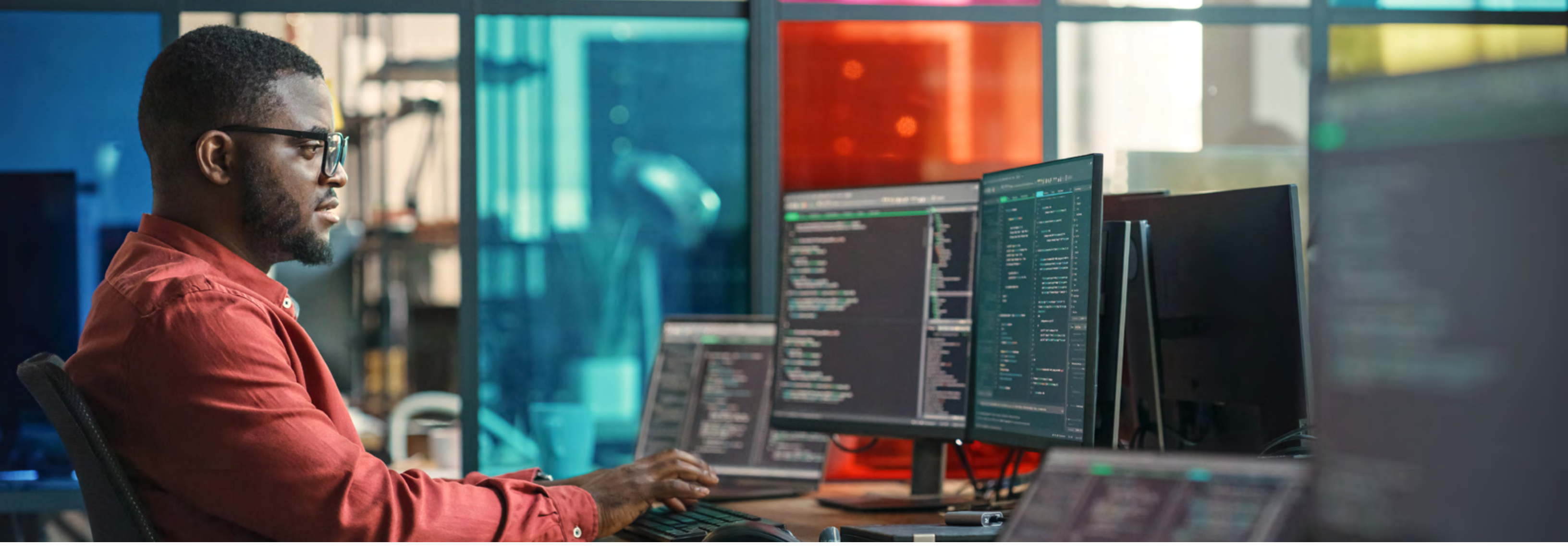
Canadian Federal Proposals

The Canadian federal government has proposed legislation with regulatory penalties as high as C$10 million and 3% of global revenue, plus fines of up to C$25 million or 5% of global revenue. A recent change to the federal proposal would allow the Privacy Commissioner of Canada to add "financial

1 Canada's National Cyber Threat Assessment 2023-2024 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.

2 2023 GLOBAL THREAT REPORT: https://www.crowdstrike.com/wp-content/uploads/2023/02/2023-Global-Threat-Report-Executive-Summary.pdf.

3 National Cyber Threat Assessment 2023-2024: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.



consideration" to compliance agreements.[4] Compliance agreements would be an alternative to fines from the to-be-formed Personal Information and Data Protection Tribunal. While this may mean lower payments, it means they will come faster and, potentially, more frequently.

This proposed federal legislation is being considered by the Standing Committee on Industry and Technology as of fall 2023 and is expected to continue to work its way through the legislative process in 2024.

Québec Privacy Law Reform

Québec recently passed significant amendments to its *Act respecting the protection of personal information in the private sector* (the Québec Privacy Act), and on September 22, 2023, the majority of those amendments came into force. The amendments impose a host of new obligations on businesses operating in Québec, and elevate Québec's privacy regime to a standard that resembles the European Union's *General Data Protection Regulation*, including the following:

— **Consequences of non-compliance**: The amendments mark a paradigm shift in how privacy law non-compliance is addressed, as it creates new penalties for non-compliance, including sizable monetary penalties against organizations and individuals. Under the new regime, the governing authority has the power to impose: (i) penal fines (as high as C$25 million or 4% of worldwide turnover for the preceding fiscal year, whichever is higher), which can be doubled for repeat offences; (ii) administrative monetary penalties (up to C$10 million, or 2% of worldwide turnover for the preceding fiscal year, whichever is higher); and (iii) civil damage awards (up to C$1,000 as punitive damages where infringements result from a gross fault).

— **Privacy by default**: Businesses are now required to ensure that their privacy settings are, by default, set to provide the highest level of confidentiality without intervention by the individual.

— **Privacy impact assessments**: Businesses are now obligated to perform a privacy impact assessment (PIA) for any project to acquire, develop, or overhaul an information system or electronic service delivery system involving personal information. Further, businesses are now required to conduct PIAs before any personal information collected in Québec can be communicated outside of the province.

— **Incident management and reporting**: The amendments introduce significant new cyber incident management and reporting requirements for businesses. Businesses must promptly notify the governing authority, as well as any other person whose personal information was affected, of an incident that poses a "risk of serious injury."

— **Data subject rights**: Individuals in Québec can exercise new rights with respect to their personal information, including requests for access, rectification and de-indexation/re-indexation/cessation of dissemination. Also, in 2024 a further right to data portability will be available.

— **Automated decision-making**: Businesses that use personal information to render decisions based exclusively on automated processing must now inform the individual about that automated decision-making, and the individual has the right to request and receive information related to the personal information used to render the decision and the reasons and the principal factors and parameters that led to the decision.

4 Government proposals to amend CPPA and AIDA: the good, the bad, and the challenges ahead Part 1: https://barrysookman.com/2023/10/15/government-proposals-to-amend-cppa-and-aida-the-good-the-bad-and-the-challenges-ahead-part-1/.

— **Governance and accountability**: There is a requirement to maintain governance policies and practices aimed at protecting personal information, which need to be proportionate to the nature and scope of their activities. Such policies at a minimum must: (i) set out roles and responsibilities of personnel; (ii) provide a framework for retention and destruction (or anonymization) of personal information; and (iii) provide a process for dealing with complaints.

— **Additional transparency requirements:** The amendments introduce increased transparency requirements, which include informing individuals of: (i) the purpose for which their information is collected; (ii) their rights of access and rectification; (iii) their right to withdraw consent to the communication or use of the personal information collected; (iv) names and/or categories of third parties who will have access to the information; (v) if applicable, how the organization collects personal information using technology that profiles, locates or identifies the individual and how to activate such technology; and (vi) the possibility that the information could be communicated outside Québec.

The amendments to the Québec Privacy Act align with the global trend of governments increasingly adopting a stringent stance on data protection to safeguard individuals in an increasingly digital world. For 2024, we anticipate businesses will continue their push to bring their Québec operations into full compliance with the new obligations to avoid being subject to the significant fines and penalties that may be levied.

Canadian Privacy Caselaw: Meta's Victory Against the Federal Privacy Commissioner

The Federal Court of Canada's recent decision in *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2023 FC 533 represents a material development in Canadian privacy law. The Federal Court dismissed a high-stakes application brought by the Privacy Commissioner of Canada (Commissioner) against Meta Platforms Inc. (formerly Facebook Inc.), which was represented by McCarthy Tétrault. This decision marked the first time any court in the world has ruled on the merits of a case arising out of the Cambridge Analytica incident.

BACKGROUND

In March 2018, the Commissioner, who oversees compliance with the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), received a complaint asking him to investigate Meta's compliance with PIPEDA in relation to Meta's sharing of personal information with third-party apps around the time of the Cambridge Analytica incident. After an investigation, the Commissioner issued a non-binding report of findings, concluding that Meta failed to get meaningful consent from Facebook users whose personal information was shared with third-party apps, and failed to adequately safeguard Facebook users' personal information from unauthorized collection, use, and disclosure by third-party apps.

Based on this report, the Commissioner filed a Federal Court application in 2020 seeking sweeping remedies that would require Meta to change Facebook's worldwide

operations and functions and to submit to ongoing supervision by the Commissioner and the court. He alleged that Meta breached federal privacy law in connection with the Cambridge Analytica incident and Meta's sharing of Facebook users' personal information with third-party apps. The Commissioner asked the court to draw inspiration from a 2019 U.S. Federal Trade Commission settlement order requiring Facebook to pay a US$5 billion fine and submit to 20 years of mandatory injunctive relief and third-party monitoring.

DECISION

Following a multi-day hearing, the Federal Court dismissed the Commissioner's application in its entirety, with costs to Meta. On both consent and safeguards, the court found no breach of PIPEDA. It also gave valuable direction on PIPEDA's interpretation and application.

PIPEDA governs the collection, use, and disclosure of personal information in Canada's private sector. Among other things, PIPEDA generally requires private sector organizations operating in Canada to do two things:

— the consent duty — obtain meaningful **consent** to collect, use, or disclose Canadians' personal information; and

— the safeguarding duty — take adequate steps to **safeguard** personal information in the organization's possession against unauthorized collection, use, or disclosure.

The court provided guidance on how to interpret and apply PIPEDA. The court noted that PIPEDA expressly aims "to establish a balance between protecting user information and an organization's right to reasonably collect, use or disclose personal information." The court stated that "given the purpose of PIPEDA is to strike a balance between two competing interests, the Court must interpret it in a flexible, common sense and pragmatic manner."

CONSENT

The court held that the Commissioner did not meet his evidentiary burden to prove that Meta failed to obtain meaningful consent from Facebook users. The court stated that even though the Commissioner enjoyed broad investigatory powers to compel information, the Commissioner's application proceeded in an "evidentiary vacuum." For example, the Commissioner failed to lead any expert evidence about what Meta could feasibly do differently to obtain users' consent, or any evidence from any Facebook users about their expectations. In the face of this evidentiary vacuum, the court declined to "speculate and draw unsupported inferences."

SAFEGUARDS

The court held that the Commissioner also failed to meet his evidentiary burden to prove that Meta failed to adequately safeguard Facebook users' personal information. The court accepted that Meta's duty to safeguard personal information in its possession ends once Meta discloses the information to a third party such as a third-party app developer. The court added that even if Meta's safeguarding duty continued after this disclosure, the Commissioner failed to show that Meta could not rely on third-party app developers' contractual commitments to comply with Facebook's terms.

KEY GUIDANCE

The Federal Court's decision provides important lessons and guidance for businesses about Canadian privacy law:

— **PIPEDA strikes a balance:** Canada's federal private sector privacy law strikes a balance between individual and organizational interests. This means courts must consider not only the individual's privacy interests, but also the organization's legitimate interests in collecting, using and disclosing personal information for commercial purposes.

— **Speculation cannot substitute for evidence:** Even if the Commissioner finds that an organization breached PIPEDA at the investigatory stage, the Commissioner bears the burden of proving the case afresh through concrete evidence on a court application. The Court will not afford any deference to the Commissioner's findings.

— **The safeguarding duty ensures seamless protection:** An organization has a duty to safeguard information in its possession. When the organization discloses the information to a third party with consent, the safeguarding duty passes from the organization to the third party immediately upon disclosure.

BUSINESS IMMIGRATION AND GLOBAL MOBILITY

Business immigration and global mobility remain important facets in the growth of Canada and its economy, specifically in the technology and innovation industries. The federal government announced plans to welcome more than 500,000 immigrants in each of 2025 and 2026, an increase of approximately 50,000 immigrants when compared to 2024. While it is an ambitious plan, it is unlikely to address the recognized shortage of skills the country is currently facing. Immigration, Refugee and Citizenship Canada (IRCC) has responded by creating specialized pathways and facilitated processes to more immediately address specific labour gaps and attract top talent in growing industries, particularly tech.

Updates Affecting Temporary Foreign Workers: New Programs to Attract Tech Talent to Canada

The lack of U.S. regulatory reform has created opportunities for Canada to benefit from the highly skilled temporary workforce that may have limited pathways to extend their status in the U.S. or adjust to U.S. landed permanent resident (LPR) status. In 2023, the Immigration Minister announced Canada's first Tech Talent Strategy. The Strategy's goal is to continue to attract individuals who have the vision and talent to establish Canada as the world leader in emerging technologies.

There are two new streams for temporary foreign workers that will drive highly skilled technology talent to Canada.

First, IRCC has announced the creation of a new exemption from the Labour Market Impact Assessment (LMIA) process to help high-growth employers and talented workers provide support to Canada's innovation priorities and high-tech industries by the end of 2023. There will be two categories:

— employer-specific work permits (valid for up to five years) for workers destined to work for a company identified by the government of Canada as contributing to industrial innovation goals, and

— open work permits (valid for up to five years) for highly skilled workers in select in-demand occupations.

This new program is groundbreaking as it extends the validity period for work permits, offering employers and foreign nationals greater certainty and stability, while also reducing the need for renewals and alleviating IRCC's processing demands. Foreign nationals with closed work permits will have a longer runway to gain Canadian work experience and accumulate points in support of their permanent residence applications.

Second, in 2023, Canada launched the H-1B visa holder work permit category where eligible H-1B specialty occupation visa holders in the U.S., and their immediate family members, may apply to come to Canada. This program offers an adaptive alternative to the difficulties that H-1B visa holders experience in extending their stays beyond six years and the significant wait times required to obtain LPR status. The program facilitates the development of an expanded talent pool, while also allowing highly skilled foreign nationals to gain Canadian work experience. Approved applicants will receive an open (i.e., non-employer

specific), work permit of up to three years, and their spouses and dependants will also be eligible to apply for accompanying documents. The program cap of 10,000 applications was met by July 2023, demonstrating the program's popularity and speaking to the possibility of similar programs in the future.

Updates to Canada's Permanent Residency Selection Process

Since the creation of Express Entry in 2015, IRCC has only conducted two types of invitation rounds:

— "general rounds," which are open to all applicants in the pool, and

— "program-specific rounds," which are open only to candidates eligible for a particular program.

Neither of these types took into account an applicant's area of professional experience or field of academic training.

In 2023, a third type of invitation round was introduced: "category-based rounds." In these, IRCC plans to invite candidates who have work experience in particular occupations, training in specific academic fields or the ability to communicate in one of Canada's two official languages. The aim is to increase invitations for those candidates working in fields affected by labour shortages. For other candidates, the "general rounds" and "program-specific rounds" continue to take place.

For 2023, IRCC announced certain categories of candidates that will be targeted in "category-based rounds," including the category of Science, Technology, Engineering and Math (STEM) occupations.

Interestingly, candidates in category-based rounds perform significantly lower than those in general rounds when assessed on their Comprehensive Ranking Score. This clearly demonstrates the government's awareness that a trade-off exists between a candidate's skills/education and other criteria.

IRCC hopes that this new policy will make Express Entry more responsive to society's changing economic and labour market needs, and in the federal government's words, act as "a catalyst for growth."[5]

Updates to the Startup Visa Program

Canada's Tech Talent Strategy also features an update to the Startup Visa (SUV) program. This update allows those with a viable business idea who are supported by a designated organization to develop their businesses in Canada and to obtain Canadian permanent resident status. Designated organizations include venture capital firms, angel investor groups and business incubators. Founders are eligible for a temporary work permit once accepted by a designated partner organization — they do not have to wait for the permanent residence process to complete.

These changes better align the SUV program with the realities of being a founder and the flexibility required to bring a vision to life. These include:

— increased availability (the program is tripling its numbers in 2023 to approximately 3,500 with further increases in 2024 and 2025);

— three-year work permits (allowing for longer term business planning and a larger variety of financing options);

— open work permits not being tied to a specific company (allowing companies to restructure as they grow without the need to update work permits, and providing the capacity for earning supplemental income if needed);

— work permits being available to the full founder team (supporting better collaboration); and

— application processing that prioritizes businesses supported by capital commitments, or incubators who are members of Canada's tech ecosystem (giving investors faster, more reliable returns on their capital).

5 https://www.canada.ca/en/immigration-refugees-citizenship/news/2023/05/canada-launches-new-process-to-welcome-skilled-newcomers-with-work-experience-in-priority-jobs-as-permanent-residents.html.

Part II: Considerations For Tech Companies Exploring Financing And Exit Options

VENTURE MARKET UPDATE

2023 Venture Market Continued to Correct From 2021 Exuberance

The significant valuation correction that hit the venture market in 2022 appears to have bottomed out in 2023. The median late-stage valuation declined by over half from its 2021 peak before starting to rebound in the first half of 2023. Average angel-, seed-, and early-stage valuations have remained more robust, and even inched upwards in certain verticals, despite lower deal volumes.

The correction came as an aftermath to the exuberance that defined the 2021 market, when historically low interest rates ushered crossover investors into the venture market in search of higher returns. Venture dollars invested nearly doubled, and valuations ballooned in the capital-rich environment. Easy private capital or bridge rounds (discussed below) caused some pre-IPO companies to push off exits and further inflated late-stage valuations.

As interest rates increased to combat rising inflation, public tech valuations plummeted in 2022 and many non-traditional investors retreated. The depressed public market and softened investor demand caused downward pressure on venture iCanada valuations, leaving companies that are close to exiting most exposed. Flat and down rounds became more common, accounting for approximately half of all financing transactions in early 2023.

However, with large amounts of venture capital (VC) cash in reserve and moderating inflation likely to slow or halt interest rate increases, 2024 is set to be a turnaround year for the Canadian venture market as it settles into a new post-correction normal.

Bridge Rounds and Layoffs Used to Extend the Runway

Convertible bridge rounds rose dramatically in the first half of 2023, as companies sought to extend their runway and avoid crystallizing lower valuations. What companies got from convertibles in avoiding down rounds, they often paid for with shortened maturities and increased interest rates. Non-dilutive sources of capital were also more aggressively sought, with elevated deal counts despite lower overall deal value. Canadian companies are increasingly lining up for funding from Canada's superclusters, where C$750 million has been earmarked for Canada's innovation ecosystem.

Internally, companies extended their runway through layoffs. Over a third of U.S. unicorns have implemented layoffs since 2022. But notably, in the years prior to 2022, many U.S. startups hired to excess and created lavish incentives, while also 'talent squatting' — essentially preventing this same talent from working for competitors. Canadian entrepreneurs were less involved in the over-hiring of 2020 and 2021 and are now capitalizing on the influx of talented candidates into the labour market. Changes to Canadian law further limiting non-compete and non-solicit provisions have further contributed to the additional mobility of startup labour.

A focus on increased revenue generation was also used by companies to reduce their burn rate and jockey for favour among investors increasingly focused on profitability versus growth. The operating margins of VC-backed companies are set to exceed their 2020 peak and the average burn rate — compared to dollar-of-revenue-generated — was reduced by a quarter.

Down Rounds: Valuation Resets Prevail Amid General Shift to Investor-Friendly Terms

Reducing burn rate and relying on bridge financing could only ever be a time-limited solution for VC-backed companies, though their efforts are evident through the near 50% increase in time between financing rounds since 2021. With many companies that last raised at peak valuations returning to the market, a pronounced increase in down rounds was inevitable.

Down rounds, which peaked at around a fifth of deals at the start of 2023, often resulted in significant valuation adjustments, relying on aggressive pay-to-play provisions to reset liquidation stacks and encourage insider participation. To offset the near-complete dilution of common equity, many transactions included structures to top-up the equity participation of current employees and management. For directors, extra care was needed in navigating fiduciary duties and sources of liability when operating with a short runway and engaging in significant recapitalizations.

Despite the harsher fundraising environment, other investor-friendly terms — including liquidation multiples, participation, and anti-dilution provisions — did not move significantly, nor did the rate of VC-backed bankruptcies.

Valuation Trends Heading into 2024

The correction in valuations that took place across 2022 and 2023 should be seen as exactly that — a correction and not a representation of any structural weakness in the venture market. With valuations rebounding near their pre-2021 levels and still significantly higher for early rounds compared to previous periods, the market is showing signs of resilience. Earlier-stage companies, which managed to escape the worst of the downward pressures over the last two years, continue to account for over 80% of venture deals. While deal volume has dropped across all stages, there has been a general uptick in deal size and valuations at the early stages, demonstrating that investors are still willing to take big bets, if only more selectively.

For later-stage companies, U.S. market data suggests the after-effects of the correction may be slower to wear off. IPOs continue to be relatively unattractive, with the 2021 vintage still underperforming and new activity at its lowest point since 2009. The performance of 2023's limited tech IPOs has also been quite tepid, and median offering sizes have seen a reduction of nearly three-quarters. Company valuations at IPO, compared to total funding before IPO, show a 50% decrease in ROI.

VC-backed M&A, on the other hand, has been resilient, trailing only 2021 in volume and outperforming the broader M&A market that struggled in 2023. The prevalence of VC-backed M&A relative to IPOs hit the highest level since the 2008 global financial crisis, and M&A deals saw a smaller decline in investor ROI compared to IPOs. With additional price clarity as the venture market recovers, we expect to see additional VC-backed M&A activity and efficiency in 2024, particularly as strategic buyers seize lower valuations as an opportunity to make acquisitions at a discount.

VC-backed companies will continue to emphasize revenue generation and reduced burn rate in 2024. The correction to the venture market has resulted in a reduction of nearly half to the viable burn rate of VC-backed companies, calculated as the average amount raised over the average time between rounds. Investors have also refocused on a disciplined, profit-driven approach, a reversion from the growth-at-all-costs strategies that were the hallmark of the 2021 bull market. The frenzied rate of valuation step ups between rounds has abated, helped along by the exodus of non-traditional investors. Corporate venture

capital, however, remains notably prevalent. Despite the significant dry powder remaining in the venture market, underpinned by the historically low deployment rate of funds raised during the 2021 bull market, a funding gap of nearly 50% means companies will be eager to show strong financial management and profit potential to attract scarce VC dollars.

Unsurprisingly, AI is emerging as an investor focus for 2024, with more than a 30% premium priced into early-stage AI companies. The Canadian market has shown a particular concentration on the sector, with over half of VC dollars going to AI companies in 2023, compared to a quarter in the U.S. Despite the premiums investors are offering, they have ample supply to choose from. Heightened M&A activity involving AI companies reflects the magnitude of activity in the space and the appetite of strategics for acquiring, versus building, AI solutions. Companies that can show technical differentiators will be better positioned for long-term success. The need for an extended runway is also supporting the growing adoption of AI, as many startups look to integrate AI solutions, particularly generative AI, to amplify productivity, reduce costs and move toward profitability.

For investors, the reset of venture valuations suggests an opportunity to generate improved returns compared to investments of the past few years. Patterns emerging today are similar to those of the 2008 financial crisis. Funding for late-stage venture companies slowed, while funding at the seed stage remained persistent. New companies were funded throughout that time at a growing rate despite the slowdown in funding companies post seed. It took three years for Series A and B round amounts to reach above the volume of invested dollars in 2007. If we are to follow a similar cycle, seed-stage companies funded now will have 2021 level Series A and B round amounts by 2025.

While early-stage tech companies in Canada may find it more challenging to raise funds than in prior years, they will also find that seed-stage valuations are robust, dry powder is available, and there is an influx of affordable talent. Although some negative market conditions remain, companies with strong fundamentals are still in demand and able to raise above-average rounds. VCs will focus their attention on strong metrics, revenue generation and decreased burn rate. While there has not been pressure to deploy funds in the latter half of 2022 and 2023, savvy investors will recognize the potential value gained from investing in the current market before it heats up in 2025, and a small thaw in the venture market will unlock the enormous stores of VC dry powder.

TECH LENDING

Overview of Market Conditions

Following the pandemic boom of 2021, market conditions, including rising interest rates and general economic uncertainty, have contributed to a relatively slower tech lending market. In contrast to priced-equity rounds — which have fared better in the first six months of 2023 — the number of loans for angel-backed and seed-stage companies fell by 44%, early-stage loans fell by 45%, late-stage loans fell by 27% and venture-growth loans fell by 39%. In terms of deal value, startups across all stages in the U.S. closed approximately US$6.34 billion across 931 debt deals in the first half of 2023, compared to US$20.07 billion across 1,513 deals in the first half of 2022. Furthermore, general market uncertainty following the collapse of Silicon Valley Bank (SVB) has contributed to a decline in loan activity. Lenders are becoming increasingly more selective with respect to their investments and have placed a stronger emphasis on credit diligence and higher underwriting standards.

Impact of Silicon Valley Bank Collapse

The collapse of SVB in March 2023 has continued to affect the tech industry with the impact being felt significantly among early-stage tech companies. Historically, SVB played a role in the venture ecosystem, providing credit facilities and operating liquidity to early-stage tech companies, a segment that had historically found it challenging to obtain financing from the traditional bank market.

Despite its smaller presence here, the collapse of SVB has also affected the Canadian tech lending sector. The immediate concern, among tech companies and lenders alike, was further contagion risk in the wider banking sector, which led to fears concerning access to liquidity. The acquisition by National Bank of Canada of SVB's Canadian commercial loan portfolio in August 2023 provided a signal of confidence to the market. Market participants, however, remain cautious of any lingering impact of SVB's collapse on lender behaviour.

As a general matter, venture debt has become increasingly popular among startups as companies are able to gain access to funding without diluting shareholder equity. However, current market conditions have resulted in venture debt becoming less available to early-stage tech companies and prospective lenders now have the ability to negotiate more lender-friendly terms. From a loan documentation perspective, lenders have placed an increased emphasis on liquidity and cash flow of companies, tighter financial covenants, greater emphasis on mandatory equity raises, requirements for investor support covenants and the inclusion of warrants and equity kickers. Stricter equity-raise requirements further protect lenders by ensuring that borrowers have sufficient capitalization and investor support. However, meeting such requirements are strained by current market conditions and the difficult fundraising environment. Investor support covenants similarly reflect the desire of lenders for increased credit support and protection but can also pose a challenge for tech companies given the current VC funding climate, as VC firms may be reluctant to have additional obligations imposed upon them. The inclusion of warrants and equity kickers further reflect the desire of lenders for additional risk mitigation and enhanced security. These factors have all contributed to a decrease in deal volume in the tech lending sector, as obtaining necessary credit approvals has become increasingly challenged.

The current market has also led to tech companies utilizing venture debt to bridge their capital needs as a way to continue operations and service liquidity, while they seek alternative equity-based funding. We are also seeing an increase in refinancing requests among tech companies due to loan repayment requirements as a result of a breach of existing loan covenants.

Lending Trends Heading into 2024

Despite current economic conditions, we have seen certain market participants either entering or expanding their position in the venture-debt market. Notably, BlackRock Inc. acquired Kreos Capital, a leading provider of growth and venture-debt financing, in June 2023. In a recent market survey, 42% of respondents stated that they saw venture debt as one of the biggest opportunities in the private-credit asset class, representing a general expectation that venture lending will play a larger role in the direct lending market moving forward.[6]

In the Canadian market, various Canadian banks are similarly expanding their reach in venture-debt lending signalling confidence and support for the venture ecosystem. The SVB collapse has spurred increased activity in the Canadian venture-debt market, which can be seen through the organizational changes of certain Canadian lenders. Following the collapse of SVB, certain key strategic personnel from SVB Canada have migrated to key positions in other Canadian

6 BlackRock. "Global Private Markets Survey - Institutional." BlackRock, June 2022, **www.blackrock.com/institutions/en-gb/insights/global-private-markets-survey**.

financial institutions in their respective innovation banking divisions, which may signify perceived opportunities and growth in the market. This has been seen most recently through RBCx's appointment of multiple former SVB Canada employees to bolster the bank's ability to provide support and funding for pre-seed and seed-stage tech companies.[7]

Vancouver-based Montfort Capital and its subsidiary TIMIA Capital also teamed up with U.S.-based Arena Investors following the collapse of SVB. The group established a joint tech lending venture in June of 2023 with an initial capacity of US$100 million.[8] This venture, along with ones similar to it, are examples of the new entrants in the expanding venture-debt market. The growth of the venture-debt market continues to be robust, despite less than favourable market conditions. The additional market participants may intensify competition, potentially spurring the market into a rebound.

Certain market commentators have also stated that after a year of uncertainty, muted deals and slow growth, the market could be approaching a stabilization period — which could pave the way for further growth and opportunity[9] — and the current decline in deal volume in the venture-debt market may be approaching a levelling off point. Additionally, as part of record-high dry powder across all U.S. sectors, dry powder earmarked for the tech sector was estimated at approximately US$250 billion in January 2023.[10] While capital deployment has been muted in the current market, the amount of dry powder may be a prelude to a future robust market with increased liquidity and lender confidence.

MINORITY INVESTMENTS

As the volume of M&A transactions in the tech sector decreased in 2023, one area for fundraising that continued to show signs of meaningful activity was minority investments in high-growth companies seeking growth equity, partial liquidity for shareholders or a bridge to a potential exit transaction or IPO.

According to the Canadian Venture Capital and Private Equity Association, minority investments accounted for 42% of all private equity dollars invested into Canadian

7 RBC Royal Bank. "RBCx Steps up Support for Founders in Two High Growth Canadian Tech Segments to Fuel Startup Ecosystem Growth & Innovation." www.newswire.ca, 1 Nov. 2023, www.newswire.ca/news-releases/rbcx-steps-up-support-for-founders-in-two-high-growth-canadian-tech-segments-to-fuel-startup-ecosystem-growth-amp-innovation-874543301.html.

8 Scott, Josh. "Montfort's TIMIA Capital, Arena Investors Aim to Fill SVB Gap with New $100 Million USD Venture | BetaKit." BetaKit, 30 June 2023, www.betakit.com/timia-capital-and-arena-investors-aim-to-fill-svb-lending-gap-with-new-100-million-usd-venture/.

9 Bradbury, Rosie. "Dealmaking Decline levels Off: US VC Trends in 5 Charts for Q1 2023." Pitchbook, 14 Apr. 2023, https://pitchbook.com/news/articles/venture-capital-monitor-charts-Q1-2023.

10 Taplin, Steve. "Council Post: What Is Dry Powder, and How Will It Affect Technology in 2023?" Forbes, 17 Mar. 2023, www.forbes.com/sites/forbestechcouncil/2023/03/17/what-is-dry-powder-and-how-will-it-affect-technology-in-2023/?sh=53cfa2eb1af.

companies in Q1 2023, and the tech sector accounted for a significant portion of those dollars.

Private equity sponsors and growth equity funds have been instrumental in driving the uptick in minority stakes in Canadian tech companies, particularly with a proliferation of tech-focused private equity funds in the U.S. and abroad that are still holding onto unprecedented amounts of dry power after recent record fundraising years. With private equity firms feeling challenged to do full buyouts in 2023 due to the broader macroeconomic environment and rising interest rates, minority investments have become an attractive option for many investors, especially funds that have mandated capital allocations for such investments and diverse investment strategies. Minority investments require less capital than buy-out transactions, can often be financed from cash calls without taking on significant debt, provide a toehold in many companies on the path to an exit and frequently have attractive features such as rights of first offer on future transactions.

Strategics have also been making an increasing number of minority investments, particularly as many of the large tech companies were reluctant to do full M&A transactions in 2023 while conducting mass layoffs. Minority investments garner considerably less attention from the public and can often be accompanied by important strategic and commercial arrangements, such as exclusive licences and collaboration agreements. Furthermore, many strategics are also holding onto unprecedented levels of cash on the balance sheet and are seeking deals that will attract less regulatory scrutiny in an increasingly aggressive regulatory environment. Emerging Canadian tech companies are often very receptive to overtures from U.S. strategics (even at reduced valuations) to provide validation and a champion for the critical U.S. market.

For target companies, minority investments have the benefit of bringing cornerstone investors onto the capitalization table and providing a bridge to a potential M&A transaction (particularly as more controlling shareholders are waiting until valuations stabilize or improve). Existing shareholders may also be able to realize partial liquidity through a minority investment if the transaction is set up with both primary and secondary components, or with special dividends from primary proceeds.

Based on our experience, key legal trends for 2023 included the following:

— Fewer private equity firms and strategics are seeking board appointment rights, observer status or even board-level information rights. Typically, such rights are afforded to important anchor shareholders that have at least a 10% equity position in the company. In the past, investors would sometimes forego these rights due to concerns about director liability, confidentiality walls and fiduciary duties that could constrain the appointing investors. However, in 2023, investors increasingly cited regulatory concerns when foregoing these rights.

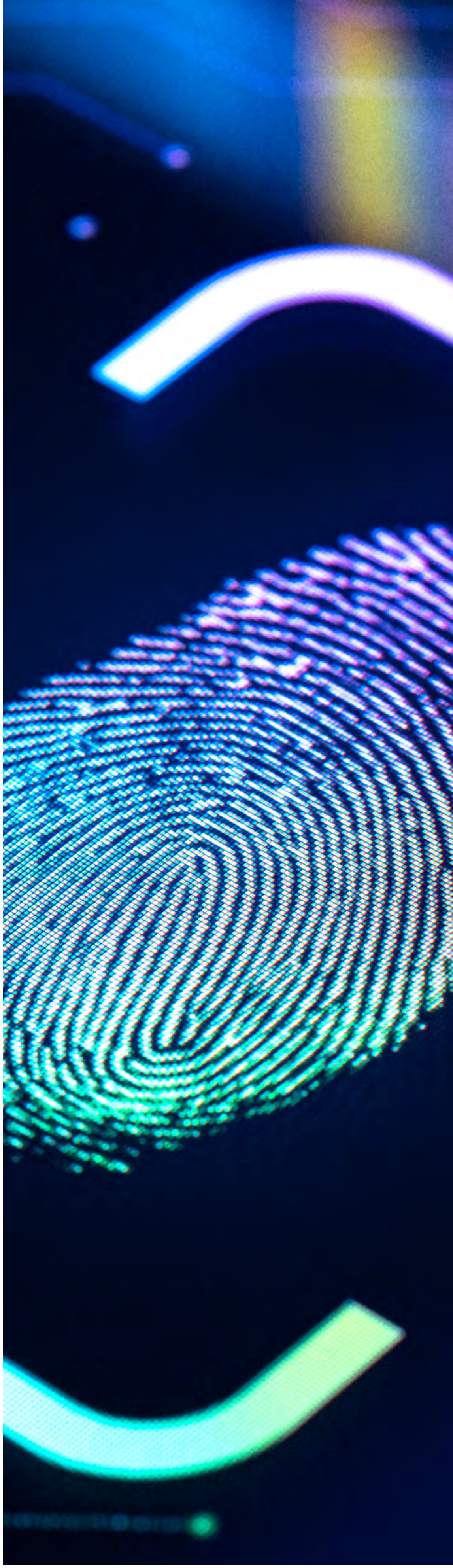
- Minority investors are scaling back the extent and scope of veto rights. Whereas in the past, investors would often ask for the "kitchen sink" for financial, strategic and operational matters, there are increasing concerns that these rights could be viewed as a form of control or significant influence that would also attract the scrutiny of regulators. The regulatory ire is not limited to Canada, as global regulators (particularly in the EU) have adopted far-reaching regulations that could apply to Canadian companies doing business there.

- More minority investors are pushing for aggressive structured liquidity rights, such as put rights and forced sale provisions. These have become a common ask by anchor minority investors, particularly as more companies paused exit or liquidity events for their shareholders based on market conditions.

- In cases where minority investors are being forced into an exit transaction (such as, for example, in a drag-along sale transaction), private equity minority investors are increasingly asking for threshold protections that allow them to achieve a minimum internal rate of return or return on invested capital. Financial investors have become more concerned about founders and early-stage investors pulling the trigger on an exit early or in a down market (and thereby disrupting an investment thesis), as Canadian founders and early-stage investors reduced their valuation expectations in challenging M&A and financing environments.

- Minority investments by foreign investors are attracting increased regulatory attention under the *Investment Canada Act* (ICA). The Canadian federal government has become more active in reviewing foreign investments in the technology sector under its general national security regime, under which the government can review the acquisition of even *de minimis* minority interests in a Canadian business, or in certain Canadian entities. Due to geopolitical issues and a more rigid regulatory environment globally, the Canadian government has expanded the scope of businesses and investors that it considers may raise national security issues — including technology companies with critical technology, intellectual property or personal data of Canadians — especially in respect of minority investors by investors based in certain jurisdictions. Given the broad remedial powers under the ICA, including the ability to block investments, order mitigation or order divestitures (in 2022, the government of Canada ordered certain Chinese companies to divest of their minority equity interests in three publicly traded Canadian lithium mining companies), foreign investors should take note of this trend.

Based on consensus forecasts that still expect a challenging first half of 2024 for Canadian tech M&A, we expect that investors will continue to gain leverage negotiating minority investments and that deal terms will become increasingly investor friendly.



ANTITRUST AND FOREIGN INVESTMENT CONSIDERATIONS FOR TECH COMPANIES PURSUING M&A

Global Antitrust Tackles Tech M&A

The requirement to canvass potential global antitrust filings in the context of an M&A event is not new. However, two increasing trends in recent years should be kept in mind as they can cause an unexpected impact on Canadian tech M&A.

First, Canadian tech companies are becoming increasingly more global — whether through sales to customers around the globe, or some other kind of global presence (e.g., employees working remotely in different countries). Second, a number of jurisdictions around the world have broadened their antitrust legislation to cover the acquisition of all kinds of tech companies, even where the target has little or no revenues in that jurisdiction. These two things taken together expand the scope of global antitrust laws that may be triggered in the context of an M&A event for a Canadian tech target — often to the surprise of buyers and sellers.

For example, both Austria and Germany have revised their antitrust regime with the intention of capturing transactions involving targets with no, or insignificant, revenue in the jurisdiction, but that nonetheless have a significant presence. In 2021 the European Commission issued new guidance under the EU Merger Regulation that expanded the conditions under which the European Commission would review a transaction referred to it by a member state and highlighting the trend of increased concentration by firms in the digital economy despite their generating little or no turnover. In 2022, the Turkish Competition Authority amended its legislation to broadly cover acquisitions of companies active in certain industries (including digital platforms, software and financial technologies) that operate, carry out R&D activities or offer services to users in Turkey. In 2022, the Japan Fair Trade Commission announced the creation of a new office specializing in market analysis for the review of tech sector mergers.

The discovery of a required antitrust requirement late in the negotiation process can upset transaction timelines or put stress on carefully crafted risk allocations. For these reasons, it is critical for both buyers and sellers of Canadian tech targets to be alive to these issues as early as possible in the M&A process.

Investment Canada Act Update: Amendments Focus on Protection of Intellectual Property and Personal Data

In December 2022, the Canadian government introduced Bill C-34: *An Act to amend the Investment Canada Act*. The bill, which would introduce comprehensive changes to the national security review regime set out in the ICA and which represents the first significant changes to the ICA since the introduction of the national security regime in 2009, indicates the government's increased focus on national security and economic security issues, including preventing sensitive Canadian intellectual property and know-how from being accessed by undesirable foreign investors (and governments).

The existing ICA sets out two parallel regimes: the "net benefit" regime and the national security review regime. The "net benefit" regime sets out a mandatory filing requirement for all acquisitions of control of a Canadian business, and for greenfield establishments of new Canadian businesses. Acquisitions of control that exceed specified financial thresholds are subject to a pre-closing application for review filing and approval requirement, which requires the investor to demonstrate that the investment is of "net benefit" to Canada; while acquisitions of control that do not exceed the applicable

threshold, and new business establishments, are subject only to a mandatory notification requirement, which can be submitted prior to or within 30 days after closing.

The national security review regime allows the Minister of Innovation, Science and Industry (the Minister) to order a review of any transaction that is subject to a mandatory filing obligation (i.e., acquisitions of control of and establishments of Canadian businesses), as well as any transaction involving an acquisition of an interest in, or in certain cases assets of, an entity that carries out operations in Canada and has a place of business in Canada, assets in Canada or individuals employed in connection with the entity's operations in Canada. Investors with transactions that fall into the broad category of transactions that are subject to national security jurisdiction but not a filing requirement may choose to make a voluntary notification prior to or within 30 days after closing.

Among other changes, Bill C-34 would implement a mandatory pre-closing notification requirement for certain investments in businesses that carry out "prescribed business activities," which result in the investor obtaining access to — or the ability to direct the use of — "material, non-public technical information or material assets," and the investor would have the power to appoint a board member, senior manager, trustee, or general partner, or would have "prescribed special rights." While the prescribed activities have not yet been defined, the government's existing *Guidelines on the National Security Review of Investments*[11] indicate a number of technology-focused areas that are considered sensitive for national security purposes, including AI, biotechnology, neurotechnology, quantum science, robotics, and space technology. Accordingly, it is likely that upon the coming into force of Bill C-34, an increased number of technology acquisitions with a nexus to Canada will be subject to a pre-closing filing requirement.

Further emphasizing the concern surrounding technology development and know-how in Canada, Bill C-34 also would expressly require the Minister to consider the effects of an investment in intellectual property developed or funded by the Canadian government, and the use of personal information about Canadians. These provisions indicate that Canada's foreign investment regime, too, is shifting its spotlight to technology acquisitions.

As of publication, Bill C-34 has not yet been passed and the timeline for its coming into force is not clear. However, the proposed amendments add another layer of complexity for non-Canadian investors contemplating investments in the technology sector in Canada.

TECH M&A TARGETS WITH LARGE AND COMPLEX CAP TABLES

Executing M&A for privately held Canadian tech targets has become increasingly complex over the past decade. Ever-increasing amounts of private capital available to fund growth, as well as increased dependence by many companies on equity compensation to reduce cash burn in the current challenging environment, means this is a trend that will continue.

A successful company may have undertaken multiple-priced rounds of equity financing resulting in multiple classes of shares with differing share rights and liquidation preferences. It may have granted equity incentives like

11 https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/guidelines/guidelines-national-security-review-investments.

stock options, RSUs, or even management carve out rights as compensation to a large number of employees and contractors in order to attract and retain the best talent. And it may have issued warrants and equity sweeteners to lenders and other commercial counterparties. By the time the company reaches the point where founders and investors are ready to exit, the capitalization table may be large, complex and unwieldy.

All of this leads to the importance of the parties turning their minds to structuring as early as possible in the pursuit of an M&A buyout. Although the sell-side will represent that the buyer is acquiring 100% of the target company, these considerations are typically as much a buy-side issue as both buyers and sellers will want to minimize execution risk, while pursuing the overall goal of a successful closing as efficiently and predictably as possible. Structuring the acquisition of a target with a complex cap table typically leads to an analysis of potential drag-along rights in the company's shareholder agreements and, increasingly, whether the benefits of using a plan of arrangement outweigh the costs.

Drag-Along Considerations

Most privately held tech companies have a shareholders' agreement in place, which provides for drag-along rights. Equivalent provisions covering holders of equity incentives like stock options and RSUs are often either included in the shareholder agreement or covered separately in the applicable equity incentive plans. Drag-along rights are often framed as a mechanism to enable majority shareholders to force the rest of the securityholders to participate with the majority in a sale of the company; however, depending on the terms and conditions of the drag-along rights, their existence can be beneficial to all parties to a transaction, including minority securityholders. This is because such rights often contain protections for the benefit of minority securityholders, while providing majority shareholders and buyers with a mechanism for completing an efficient and predictable sale of the target company.

The prevalence, and perceived utility, of drag-along rights often result in parties deciding early in a sale process that reliance on a drag-along right is the best mechanism to not only ensure that all securityholders are required to support the transaction, but also to facilitate the transaction's closing by avoiding the need to track down each and every individual securityholder for approvals and/or signatures on deal documents. While the existence of drag-along rights can achieve that objective, it is imperative that parties review the specific terms and conditions of drag-along rights, against the terms and conditions of the sale transaction, as well as turn their minds to enforceability considerations. Importantly, that review should continue as deal terms will typically evolve during negotiations. Key questions parties should turn their minds to when deciding whether the drag is workable include the following:

— Does the drag-along provision give a representative of the majority shareholders, or the target company, a proxy to vote and/or a power of attorney to sign all customary deal documents on behalf of the dragged securityholders? If so, have all of the securityholders who are to be dragged signed on to the relevant document containing the drag-along right? If the answer is no to either of these questions, the drag-along provision may not provide a complete solution for achieving an efficient and predictable M&A closing.

— Does the transaction go beyond a straightforward sale of all shares or assets of a target company? Where the deal involves additional elements requiring

shareholder participation (e.g., certain pre-closing reorganizations), parties should consider whether the drag-along provision covers those additional elements, and if not, how to manage any approvals and/or signatures not covered by the drag-along.

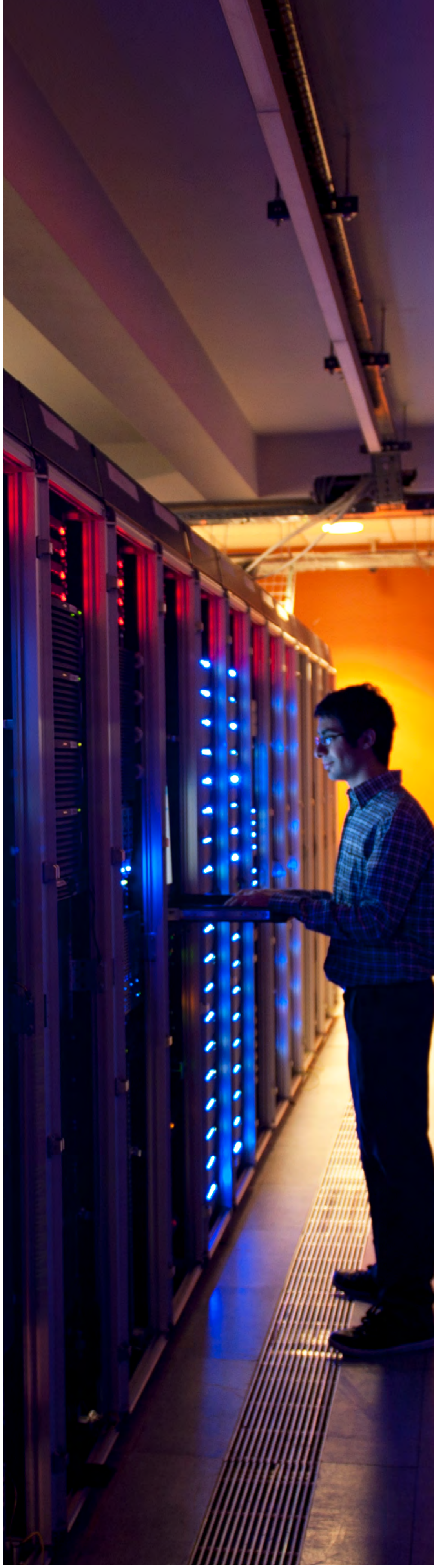
- Are all securityholders being treated equally under the M&A deal? Drag-along provisions often include, as a condition to their use, that all dragged shareholders be treated equally under the M&A deal, and some drag-along provisions extend this concept of equal treatment to holders of equity incentives like stock options and RSUs.

- To what extent will post-closing obligations of the buyer apply to all securityholders? Drag-along provisions often include, as a condition to their use, that the minority securityholders being dragged can only be subject to very narrow post-closing obligations to the buyer. These permitted post-closing obligations may not extend to the full range of obligations required under the terms of the deal.

- Is the buyer comfortable relying on the drag-along? Although whether or not to exercise drag-along rights is initially a sell-side consideration, the practical reality is that the buyer and its advisors will generally expect to have a seat at the table in making this decision. Many buyers will naturally be reluctant to rely upon forced sales by minority shareholders due to the enforceability risk and concerns about litigation.

Plans of Arrangement as a Structuring Alternative

Corporate statutes in Canada generally provide a mechanism for companies to be sold through a court-supervised process called a plan of arrangement, which has some similarities to a Delaware-style merger. The vast majority of public M&A deals in Canada are completed using this structure. However, the use of the plan of arrangement structure for the completion of the sale of privately held Canadian tech targets with large and/or complex securityholder bases is on the rise. This is because the structure can sometimes be used to achieve the sale of 100% of a target company's shares to a buyer, while avoiding the need to track down each and every individual securityholder for approvals and/or signatures on deal documents and getting a final court order approving the transaction (thereby helping minimize litigation risk, albeit while triggering dissent rights similar to U.S. state appraisal rights). Using a plan of arrangement can also achieve a number of other benefits. For example, complex reorganizations, transactions involving the issuance of the buyer's shares as consideration and the target's outstanding equity incentives can often be dealt with under the arrangement. On the flip side, using a plan of arrangement involves additional steps to completion, including court filings and appearances, and requires consideration of what information about the deal will be made publicly accessible as a result of the court process. Whether or not a plan of arrangement is the appropriate structuring solution for the acquisition of any particular privately held tech target will depend on a variety of factors; however, it has proven to be effective in situations where drag-along rights do not exist, or are not the ideal mechanism for achieving an efficient and predictable M&A closing.



M&A DILIGENCE CONSIDERATIONS FOR AI BUSINESSES

In 2022, OpenAI introduced a demo of its ChatGPT app, a chatbot that can provide answers (or ask clarifying questions) based on text prompts inputted by users. ChatGPT became an overnight sensation, attracting over one million active users within the first five days following its release and an estimated 100 million active users within the first two months following its release. With the success of ChatGPT, there has been a proliferation in the development and use of generative AI technologies, which has fuelled increased interest in investments in, or acquisitions of, AI businesses. However, the accelerated adoption of generative AI technologies has also resulted in heightened governmental and legal scrutiny, which could present unique legal challenges when prospective investors assess whether to invest in, or acquire, AI businesses.

Although the direction in which legislation and jurisprudence will take on AI remains largely unsettled, when prospective investors and acquirers in and of AI businesses conduct due diligence, they should not only be mindful of the more traditional risks associated with software-based businesses (such as risks associated with open source code, intellectual property ownership and cybersecurity), but also novel risks that are specific to AI technology, including those discussed below.

COPYRIGHT INFRINGEMENT RISK

The rise of generative AI training practices for both AI models and data sets has heralded a growing number of class action copyright infringement lawsuits, especially in the U.S.[12] The lawsuits follow a similar pattern. The plaintiffs are owners of copyrighted work. At the other end of the dispute are predominantly AI businesses, including the owners of the biggest generative AI chatbots and text-to-image generators, such as ChatGPT and Stability AI. The plaintiffs typically allege the following claims:

— **Direct copyright infringement:** The AI business has, without the plaintiffs' consent, copied and used the plaintiffs' copyrighted works to train machine learning models.

— **Vicarious copyright infringement:** The AI business has financially benefited from the infringing output of the machine learning model. As a result, every output from the machine learning model is an act of vicarious copyright infringement.

In many instances, the defendants have filed motions to dismiss the cases brought by the plaintiffs and have used "fair use" under the U.S. *1976 Copyright Act* as a defence.[13] However, to date, most of the claims remain ongoing. In one particular lawsuit brought by a group of artists against several AI companies, the U.S. federal court judge largely granted the defendants' motion to dismiss.[14] Among other reasons, the judge found that the plaintiffs failed to satisfy the basic prerequisite to file a copyright infringement lawsuit under the U.S. *1976 Copyright Act*: registration. The only claim that survived was the claim of direct copyright infringement by the one plaintiff who had registered copyright protection in her works.

Based on the current litigation landscape, when performing a legal due diligence review on an AI business, it would be prudent for prospective investors and acquirers to consider:

— to what extent the AI business has used copyrightable works in its data sets used to train any of its AI models, as doing so could attract the potential of a direct copyright infringement claim;

— to what extent users of the AI products receive output from AI models or data sets that may have been trained on copyrightable works, as doing so could attract the potential of a vicarious copyright infringement claim; and

— if any data sets used to train AI models include any of the copyrightable works that are registered with the U.S. Copyright Office, which would give the copyright owner a right to initiate a claim against the AI business under the U.S. *1976 Copyright Act*.

The liability questions posed by the recent copyright litigation will be assessed by courts for many years to come. The full scope of potential liability for developing or using AI technologies remains, like the technologies themselves, continuously evolving.

12 For example, *Getty Images (US), Inc. v. Stability AI*, Inc., 1:23-cv-00135, (D. Del.); *Andersen v. Stability AI Ltd*., 3:23-cv-00201, (N.D. Cal.) ("*Andersen v. Stability AI*"); *Tremblay v. OpenAI, Inc*., 3:23-cv-03223-AMO, (N.D. Cal.) ("*Tremblay v. OpenAI*"); *Silverman v. OpenAI, Inc*., 3:23-cv-03416, (N.D. Cal.); *Kadrey v. Meta Platforms*, Inc., 3:23-cv-03417, (N.D. Cal.).

13 For example, in support of its motion to dismiss under *Tremblay v. OpenAI*, OpenAI has argued that its use of copyrightable works with AI-driven chatbots amounts to a novel technological use that the U.S. copyright regime did not intend to suppress.

14 *Andersen v. Stability AI*, Order on Motions to Dismiss and Strike.

DATA SET RISKS

The data sets that AI companies use to train their respective AI technologies are integral to the functionality (and success) of their AI technologies and could therefore carry significant value. Accordingly, it is important to review how those data sets are consolidated or developed, and how they are being used in or with AI technologies. The following should be considered when performing legal due diligence review on AI companies:

— **Rights to training data sets**: The prospective investor or acquirer should consider: (i) if the data sets are owned by the AI business, if and to whom the data sets have been licensed; and (ii) if the data sets are owned by a third party, what rights the AI business has to use the data sets and whether the AI business will continue to have access to the data set in the event of a change of control.

— **Contents of the data sets**: The contents of the data sets could have additional legal implications. For example, if the data sets contain personal information, the prospective investor or acquirer should consider whether the personal information therein has been collected, used, disclosed, and processed in compliance with applicable privacy laws.

— **Source of data Sets**: The source of the data used in data sets could attract greater legal liability if, for example, any of the data sets were obtained from illegitimate sources or without appropriate licence rights. In these circumstances, the AI business could be exposed to greater litigation risk, as discussed above.

AI REGULATORY RISK

The rise in the use of generative AI technologies has also resulted in increased governmental scrutiny. Governments are growing increasingly concerned about the harm that generative AI technologies can cause and many countries are in the process of introducing regulatory frameworks to manage the risk associated with AI.

European Union

For example, in April 2021, the European Commission proposed the first EU regulatory framework for AI, *Laying down harmonized rules on artificial intelligence* (the *EU AI Act*). The *EU AI Act* classifies AI technologies into three main categories, based on the potential risk that the AI technologies could create. AI technologies that create a social scoring system or that are aimed to exploit children or other vulnerable groups are considered to create an unacceptable level of risk and are strictly prohibited under the *EU AI Act*. AI technologies that fall within the scope of other EU harmonized product safety legislation (and are required to undergo a third-party conformity assessment before being made commercially available in the EU) or under a prescribed category under the *EU AI Act* are considered to create a high level of risk, and providers of such AI technologies must: (i) register their AI technology in an EU database; (ii) undergo an assessment prior to making the AI technology commercially available in the EU; and (iii) comply with strict requirements, including maintaining:

— a risk management system that ensures that its AI technology is operating in a manner that is consistent with its intended purpose; and

- data governance practices that ensure that data sets used with its AI technology are error-free, accurate and consistent with design choices.

Finally, any other AI technologies that interact with people or generate image, audio or video content are considered to be low risk, and those AI technologies must comply with certain transparency requirements that enable users to interpret the technology's output and to use it appropriately. The *EU AI Act* is still under debate and has not yet been enacted.

United States

On October 30, 2023, U.S. President Biden issued an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (Executive Order), which is aimed at, among other objectives, establishing new standards for AI safety and security, promoting responsible innovation and competition and protecting consumers and privacy and civil liberties. The Executive Order imposes certain disclosure and testing requirements on AI companies that have developed AI models using a massive amount of computing power[15] or that acquire, develop or possess a potential large-scale computing cluster.[16] AI companies that meet the criteria must provide to the U.S. federal government, on an ongoing basis, information, reports or records regarding: (i) any ongoing or planned activities related to training, developing or producing applicable AI models, including the physical and cybersecurity protections used to assure the integrity of training processes used; (ii) ownership and possession of the model weights used for AI models, and the physical and cybersecurity controls used to protect against unauthorized access to those weights; and (iii) the results of any "red-teaming" tests aimed at identifying flaws or vulnerabilities in the AI model.

Canada

On June 16, 2022, the government of Canada tabled its proposed *Artificial Intelligence and Data Act* (AIDA), which is intended to impose certain requirements on "high-impact" systems, including the implementation of measures to mitigate potential harms or biased outputs that such AI technologies could produce, including controls to monitor the effectiveness of those measures and procedures to keep records relating to those measures. Although the government of Canada has released some guidance on what could constitute a "high-impact" system and some of its underlying policy goals, *AIDA* is still under debate and has not yet been enacted.

On the provincial level, as discussed in greater detail below (see **Developments in Canadian Privacy Law — Québec Privacy Law Reform**), Québec introduced significant amendments to Québec's provincial privacy laws. As a part of those amendments, Québec private businesses are now required to inform Québec residents if they use their personal information to render a decision exclusively through automated processing. Additionally, upon any applicable individual's request, the business must inform the individual of: (i) the personal information used to render the decision; (ii) the reasons and principal factors that led to the decision; and (iii) the individual's right to correct any personal information used.

AI Regulatory Due Diligence Considerations

When performing legal due diligence reviews on AI businesses, prospective investors and acquirers should

15 The requirements apply to those AI models that were trained using a quantity of computing power greater than 10^{26} integer or floating-point operations (or using primarily biological sequence data and using a quantity of computing power greater than 10^{23} integer or floating-point operations), and that are: (a) trained on broad data; (b) generally use self-supervision; (c) contains at least tens of billions of parameters; (d) is applicable across a wide range of contexts; and (e) that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matter.

16 The requirement applies to any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s and having a theoretical maximum computing capacity of 10^{20} integer or floating-point operations per second for training AI technologies.

consider whether the business would be subject to any relevant AI laws or regulations under the jurisdictions in which it would like to conduct business, including any onerous requirements, measures, and controls that the AI business may be required to implement if any proposed laws or regulations are enacted and become enforceable.

Operational Risk: Access to Infrastructure

The rise in generative AI usage has also spurred a race for access to computing power required to develop and operate AI technologies. For example, the demand for graphic processing units manufactured by NVIDIA that specializes in training AI “transformer” models has skyrocketed, resulting in a shortage of the physical hardware that is most often used to power AI technologies. As a result, many AI companies have instead turned to cloud clusters and neural nets made available by reputable cloud providers, which have installed large numbers of NVIDIA’s graphical processing units into their back-end infrastructure and provide customers with access to that infrastructure on a pay-as-you-go basis.

When performing legal due diligence reviews on AI businesses, prospective investors and acquirers should consider whether the business owns its own infrastructure or relies on third-party infrastructure to operate its business. Where an AI business relies on third-party infrastructure, the commercial contracts under which such third party makes its infrastructure available to the AI business should be more carefully reviewed to assess the impact that such reliance may have on the operations of the AI business (including, as an example, the provider’s rights to terminate the agreement, the measures used to protect against unauthorized access to the infrastructure and the measures used to ensure the continuity of the infrastructure).

HEIGHTENED CYBERSECURITY CONSIDERATIONS IN THE CONTEXT OF M&A DEALS

Although cybersecurity remains a day-to-day consideration for businesses, recent trends point to the heightened importance of cybersecurity considerations in M&A. When it comes to diligence, cybersecurity diligence is now a must, and it needs to be interdisciplinary. Supplementing technical diligence, buyers should be looking at:

— cyber insurance (or lack thereof);

— records of incidents (such as breach registers, reports to regulators and insurance claims); and

— the existence of policies and procedures — most critically incident response and business continuity planning/disaster recovery.

Although cybersecurity diligence is being taken more seriously in recent years, it is often still not taken seriously enough. A recent report[17] revealed that only 36% of respondents strongly agreed that their IT team is given time to review the target company's cybersecurity standards, processes and protocols before an acquisition.

When it comes to insurance, cyber insurers are increasing premiums and getting more selective following a period of poor loss ratios.[18] Some Canadian insurers have pulled out of the cyber insurance market completely.[19] This means that buyers may need to adjust their expectations on what insurance products have been, and will be, available for the target company. The existence (or non-existence) of cyber insurance may also factor into considerations for M&A deals that involve representation and warranty insurance.

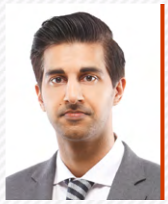
On the topic of budget allocation, Canadian organizations allocate among the lowest percentage of their operating budgets to cybersecurity of any developed country. According to one survey,[20] Canadian organizations spent, on average, 11.9% of their IT budgets on cybersecurity. While this is an increase from the reported average from the prior year of 11.1%, it still lags behind the global average of 12.7%. Buy-side diligence may need to consider the potential implications of a target company's budget allocation, or lack thereof.

In addition to diligence, buyers and sellers should be aware that threat actors may target companies involved in an M&A process, which leverages the parties' fear of exposure during the M&A process to extract payments.[21] This increased vulnerability may continue into the post-closing as the businesses work to integrate two sets of cybersecurity systems, policies and procedures.[22]

17 https://www.forescout.com/resources/cybersecurity-in-merger-and-acquisition-report/.
18 Reinsurers examining alternative ways to insure cyber: https://www.canadianunderwriter.ca/insurance/reinsurers-examining-alternative-ways-to-insure-cyber-1004238856/.
19 Can cyber coverage recover from past high loss ratios?: https://www.canadianunderwriter.ca/brokers/can-cyber-coverage-recover-from-past-high-loss-ratios-1004231846/.
20 CyberEdge Group. 2022 Cyberthreat Defense Report: https://cyber-edge.com/wp-content/uploads/2022/11/CyberEdge-2022-CDR-Report.pdf.
21 The Importance of Threat Exposure Management during the M&A Process: https://www.cpomagazine.com/cyber-security/the-importance-of-threat-exposure-management-during-the-ma-process/.
22 The Role of Cybersecurity in Mergers and Acquisitions: https://www.upguard.com/blog/the-role-of-cybersecurity-in-mergers-and-acquisitions.

FOR MORE INFORMATION, PLEASE CONTACT A MEMBER OF OUR NATIONAL, MULTI-DISCIPLINARY TECHNOLOGY INDUSTRY GROUP:

Christine Ing
Partner,
Technology Group Lead
christineing@mccarthy.ca
416-601-7713
TORONTO



Pavan Jawanda
Partner,
M&A and Private Equity
pjawanda@mccarthy.ca
604-643-7110
VANCOUVER

Heidi Gordon
Partner,
M&A and Private Equity
hgordon@mccarthy.ca
416-601-8176
TORONTO

Ranjeev Dhillon
Partner,
M&A and Private Equity
rdhillon@mccarthy.ca
416-601-8327
TORONTO

Robert Anton
Partner,
M&A and Private Equity
ranton@mccarthy.ca
416-601-8169
TORONTO

Jade Buchanan
Partner,
Privacy and Technology
jbuchanan@mccarthy.ca
604-643-7947
VANCOUVER

Stéphane Duval
Partner,
MT>iplus, Immigration
sduval@mtiplus.ca
514-397-4284
MONTRÉAL

Gillian Kerr
Partner,
Litigation
gkerr@mccarthy.ca
+416-601-8226
TORONTO

Conrad Lee
Partner,
Technology
conradlee@mccarthy.ca
416-601-7775
TORONTO

Ian Mak
Partner,
Financial Services
imak@mccarthy.ca
416-601-7528
TORONTO

Kate McNeece
Partner,
Competition/Antitrust & Foreign Investment
kmcneece@mccarthy.ca
416-601-7836
TORONTO

Aliya Ramji
Partner,
MT>Ventures
aramji@mccarthy.ca
416-601-4303
TORONTO

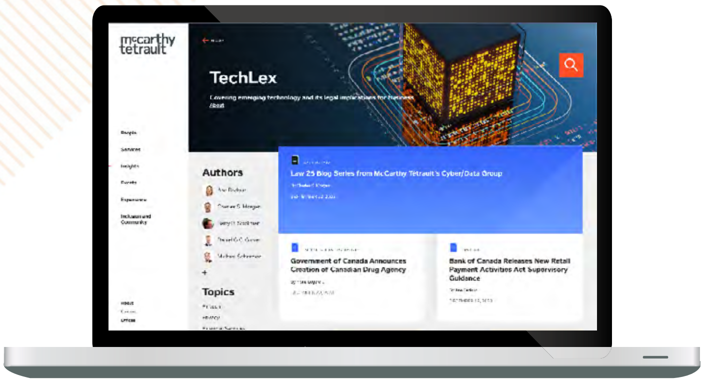
Michael Scherman
Partner,
Technology
mscherman@mccarthy.ca
416-601-8861
TORONTO

Véronique Wattiez Larose
Partner,
M&A and Private Equity
vwlarose@mccarthy.ca
514-397-4249
MONTRÉAL

A SPECIAL THANKS TO

Connor Bildfell (Associate, Litigation), John Durland (Associate, MT>Ventures), Eashan Karnik (Associate, MT>Ventures), Wendes Keung (Associate, Technology), Shefali Tanna (Associate, MT>iplus, Immigration), Vivian Sy (Associate, M&A), Juliana Smith (Articling Student) and Samantha Steeves (Articling Student).

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**

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

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